March 2001
Volume 49
Number 2

United States
Department of Justice
Executive Office for
United States Attorneys
Office of Legal Education
Washington, DC
20535

Mark T. Calloway
Director

Contributors 'opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service

The United States Attorneys ' Bulletin is published pursuant to 28 CFR § 0.22(b)

The United States Attorneys ' Bulletin is published bi-monthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201. Periodical postage paid at Washington, D.C. Postmaster: Send address changes to Editor, United States Attorneys ' Bulletin, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201

Managing Editor
Jim Donovan

Assistant Editor
Nancy Bowman

Law Clerk
Todd Hagins

Internet Address
www.usdoj.gov/usao/eousa/foia/foiamanuals.html

Send article submissions to Managing Editor, United States Attorneys 'Bulletin, National Advocacy Center Office of Legal Education 1620 Pendleton Street Columbia, SC 29201

Computer Crimes and Intellectual Property

In This Issue

Deciding Whether to Prosecute an Intellectual Property Case

David Goldstone
Trial Attorney, Computer Crime and Intellectual Property Section
Team Leader, Intellectual Property Team

Federal prosecutors know that deciding whether to prosecute a particular case requires the exercise of judgment and discretion, which can take years of experience to develop. But what if you are presented with an intellectual property ("IP") case and you have not done many of them before, if any? How should you decide whether a particular case of counterfeit computer chips, pirated music or software sold (or given away for free) over the Internet, or stolen satellite signals should be charged, even if an investigator provides evidence to prove all the elements? What special considerations, if any, come into play?

Even experienced federal prosecutors should reconsider first principles in evaluating the merits of an IP case, because of a few characteristics of such cases, including:

- IP crime always has a direct victim (the IP holder) and undermines the IP system as a whole (like counterfeiting of money), in addition to any fraud perpetrated on the recipient of the counterfeit good or pirated work;
- Because IP crime can be perpetrated without any direct contact with the victim IP holder (such as counterfeiting goods without asking the permission of the trademark holder), the direct victim of IP crime is basically defenseless against IP theft;
- IP rights, such as trademark and copyright, are in part created by federal law and administered by federal agencies and are thus of special federal interest;
- Effective enforcement of IP laws is essential to the foundation of the growing information economy; and
- The May 2000 revision to the Sentencing Guidelines more accurately recognizes the loss caused by IP crime.

The recently published manual, Computer Crime and Intellectual Property Section, Department of Justice, *Prosecuting Intellectual Property Crimes* (2001), can be a valuable resource for evaluating these, as well as the other issues that arise in IP cases. Generally, federal prosecutors should take into account the same considerations in determining whether to charge an IP crime as they would with respect to all federal crimes. *See, e.g.*, *U.S. Attorneys' Manual* § 9-27.220. Thus, the prosecutors should evaluate all the considerations normally associated with the sound exercise of prosecutorial discretion. In exercising this discretion, *U.S. Attorneys' Manual* § 9-27.220 notes three situations in which the prosecutor may properly decline to take action despite having admissible evidence sufficient to obtain and sustain a conviction for a federal crime: "when no substantial federal interest would be served by prosecution;" when [t]he person is subject to effective prosecution in another jurisdiction; "or when [t]here exists an adequate non-criminal alternative to prosecution." While individual U.S. Attorney's Offices may evaluate these factors with different standards, each of these grounds is discussed below with particular attention paid to IP crimes. Also, special considerations may arise when considering IP charges against corporations. *See Prosecuting Intellectual Property Crimes* § VI.A.4 (2001).

1. The Federal Interest in IP Crimes

In determining the substantiality of the federal interest that would be served by a prosecution, the attorney for the government should weigh all relevant considerations, including:

> (1) [current] federal law enforcement priorities; (2) the nature and seriousness of the offense; (3) the deterrent effect of prosecution; (4) the person's culpability in connection with the offense; (5) the person's history with respect to criminal activity; (6) the person's willingness to cooperate in the investigation or prosecution of others; and (7) the probable sentence or other consequences if the person is convicted.

U.S. Attorneys' Manual § 9-27.230.

All of these factors will be discussed below with specific attention to IP crimes. The last factor – the probable sentence – is especially noteworthy in light of the May 2000 revision to sentencing guideline § 2B5.3 to more accurately reflect the loss caused by IP crime. This new provision will be discussed in detail below.

a. Federal Law Enforcement Priorities

The importance of IP to the national economy, and the scale of IP theft, led the Department of Justice to designate IP crime as a "priority" for federal law enforcement. As the *U.S. Attorneys' Manual* recognizes, "from time to time the Department establishes national investigative and prosecutorial priorities. These priorities are designed to focus Federal law enforcement efforts on those matters within the Federal jurisdiction that are most deserving of Federal attention and are most likely to be handled effectively at the Federal level." *U.S. Attorneys' Manual* § 9-27.230(B)(1) (cmt).

IP crimes were formally designated a "priority" by Deputy Attorney General Eric Holder on July 23, 1999. Deputy Attorney General Eric Holder, *Remarks at Press Conference Announcing the Intellectual Property Rights Initiative* (Jul. 23, 1999) *available at* (http://www.cybercrime.gov/dagipini.html). In announcing the Intellectual Property Rights Initiative, Deputy Attorney General Holder stated that the Department of Justice, the Federal Bureau of Investigation and the United States Customs Service had concluded that they must make investigating and prosecuting IP crime "a major law enforcement priority." In making the announcement, he noted the following:

> As the world moves from the Industrial Age to the Information Age, the United States' economy is increasingly dependent on the production and distribution of intellectual property. Currently, the U.S. leads the world in the creation and export of intellectual property and IP-related products.

Deputy Attorney General Holder also observed that "[a]t the same time that our information economy is soaring, so is intellectual property theft." Since IP theft undermines the federally established copyright and trademark systems, it is especially appropriate that investigation and prosecution of these crimes be a federal law enforcement priority.

The IP Initiative is aimed at combating the growing wave of piracy and counterfeiting offenses, both domestically and internationally, with the participation of U.S. Attorney's offices in New York, New Jersey, California, Florida and Massachusetts. The initiative has focused on training activities, improved coordination among law enforcement agencies, increased cooperation with industry, and highlighting IP internationally. In September, 2000 following the first-ever meeting of law enforcement experts from G-8 countries, a group of leading industrialized nations, to discuss trends in trafficking in counterfeit and pirated merchandise, it was agreed to address trends in trans-border IP crime.

In recent years, Congress has taken an especially strong interest in IP crimes as well as IP law generally. Congress has recently enacted stiffer penalties for IP crimes, and has made many IP crimes a predicate offense under the money laundering and RICO statutes. Moreover, Congress took the unprecedented step of singling out IP crimes for detailed accounting in the Attorney General's Annual Accountability Report. In enacting the Anticounterfeiting Consumer Protection Act of 1996, Pub. L. No. 104-153, 110 Stat. 1386, Congress required the Attorney General to include in the annual report, on a district-by-district basis, the following four criteria: (1) the number of open investigations; (2) the number of cases referred by the United States Customs Service; (3) the number of cases referred by other agencies or sources; and (4) the number

and outcome, including settlements, sentences, recoveries, and penalties, of all prosecutions brought under sections 2318, 2319, 2319A, and 2320 of Title 18.

The federal interest in IP is no recent or transitory development. It has been recognized since the ratification of the Constitution. *See* U.S. Const. art. I, § 8, cl. 8. Longtime Congressional interest in providing a sound federal basis for IP law is further demonstrated by two comprehensive bodies of statutes: the Copyright Act of 1976 (codified as amended at Title 17); and the Lanham Act (codified as amended at 15 U.S.C. §§ 1051-1127). In fact, the Copyright Act in 1976 established federal preemption over state law because of the importance of a uniform federal copyright law. *See* 17 U.S.C. § 301.

b. The Nature and Seriousness of the Offense

IP crimes, like other crimes, vary in their nature and seriousness and it is therefore essential to consider each case on its own facts. Limited federal resources should not be diverted to prosecute inconsequential cases or cases in which the violation is only technical. Prosecutors may consider any number of factors to determine the seriousness of an IP crime, including:

1. Whether the counterfeit goods or services present potential health or safety issues (*e.g.*, counterfeit medications or airplane parts);
2. The scope of the infringing or counterfeiting activities (*e.g.*, whether the subject infringes or traffics in multiple items or the infringes upon multiple industries or victims), as well as the volume of infringing items manufactured or distributed;
3. The scale of the infringing or counterfeiting activities (e.g., the amount of illegitimate revenue and any identifiable illegitimate profit arising from the infringing or counterfeiting activities based upon the retail value of the infringed item);
4. The number of participants and the involvement of any organized criminal group;
5. The scale of the victim's loss or potential loss, including the value of the infringed item, the size of the market for the infringed IP that is being undermined (*e.g.*, a best-selling software package or a famous trademark), and the impact of the infringement on that market;
6. Whether the victim or victims took reasonable measures (if any) to protect against the crime; and
7. Whether the purchasers of the infringing items were victims of a fraudulent scheme, or whether there is a reasonable likelihood of consumer mistake as a result of the subject's actions.

c. The Deterrent Effect of Prosecution

Deterrence of criminal conduct is one of the primary goals of the criminal law. Experience demonstrates that many infringers will not be deterred by civil liability, which can be treated as a cost of doing business. For example, even when a permanent injunction or consent decree is in force, they do not necessarily deter some defendants. Some defendants may respond to such civil remedies by changing the item upon which they are infringing, such as counterfeiting shirts bearing marks of Major League Baseball teams after being the subject of an injunction obtained by the National Football League. Others close shop only to quickly reopen under a different corporate identity. Criminal prosecution can better deter a violator from repeating his or her crime.

Criminal prosecution of IP crimes is also important for general deterrence. Many individuals may commit intellectual property crimes not only because they can be relatively easy to commit (such as copying music) but also because the subjects believe they will not be prosecuted. Criminal prosecution plays an important role in establishing public expectations of right and wrong. Even relatively small scale violations, if permitted to take place openly and notoriously, can lead other people to believe that such conduct is tolerated in American society.

While some cases of counterfeiting or piracy may not result in provable direct loss to the holder of the IP right, the widespread commission of IP crimes with impunity can be devastating to the value of such rights. The importance of general deterrence is easily understood with regard to counterfeiting of United States currency. Even though some counterfeit bills can be "passed" without any harm to the monetary system of the United States, widespread commission of counterfeiting would be devastating to the value of the dollar. Today's brands have currency only to the extent that anticounterfeiting laws are enforced.

Vigorous prosecutions can change the counterfeiter's calculus. If individuals believe that counterfeiters will be investigated and prosecuted, they will be deterred. Industry groups representing victims of IP crimes are acutely aware of their need for law enforcement protection for IP. These victims will vigorously publicize successful prosecutions. The resulting public awareness of effective prosecutions can have a substantial deterrence effect.

d. The Individual's Culpability in Connection with the Offense

IP crimes are often committed by multiple individuals working in concert, such as a company that traffics in counterfeit goods or pirated software. *See Prosecuting Intellectual Property Crimes* § VI.A.4 (2001) (discussing special considerations for cases involving corporations). The individuals in such an organization are not necessarily equally culpable. For example, a prosecutor may reasonably conclude that some course other than prosecution would be appropriate for a relatively minor participant. In considering the relative culpability of specific individuals within a group of people who commit IP crimes in concert, a number of non-exclusive factors have proven helpful, including: (1) whether the person had oversight responsibility for others; (2) whether the person specifically directed others to commit the offense; (3) whether the person profited from the offense; (4) whether the person was specifically aware of the wrongful nature of the activity, as evidenced by the receipt of a warning such as a "cease and desist" letter or by a statement to collaborators admitting wrongfulness, but nonetheless continued to engage in the activity; and (5) whether the person took affirmative steps, such as creating misleading records, to deter investigation, and thereby facilitate commission of the offense. Other factors may also be relevant in particular cases.

e. The Individual's History with Respect to Criminal Activity

The subject's history with respect to criminal activity will of course be extremely fact dependent. Experience with IP crime cases teaches that defendants often have a history of engaging in a pattern of fraudulent conduct not necessarily limited to IP crimes. It should not be assumed that commission of an IP crime is an exception to an otherwise law-abiding life. It is appropriate to consider whether there is a reasonable basis to believe that the person has engaged in previous IP violations. A prosecutor, an investigator or a victim may be aware of a permanent injunction or consent decree in any civil case against the defendant.

f. The Individual's Willingness to Cooperate in the Investigation or Prosecution of Others

A defendant's willingness to cooperate will depend on the individual. Nevertheless, it is important to recognize that in IP cases, defendants often have a substantial capacity for cooperation, if they are, in fact, willing. Since IP crimes often require special materials, equipment, or information, and can involve multiple participants, defendants often can provide substantial assistance. This cooperation can take at least three forms. Most commonly, a defendant might cooperate in the investigation or prosecution of others directly involved in the same criminal scheme.

Second, a defendant might also provide valuable cooperation concerning the source or destination of counterfeit goods or pirated works. For example, if a defendant is investigated for selling counterfeit watches on a retail basis, he could provide information as to the wholesaler of those counterfeit watches. The wholesaler, in turn,

could provide information regarding the manufacturer, or about other retailers.

Third, a defendant might also provide information concerning the trafficking of counterfeit packaging materials in which counterfeit goods may be sold. This information is easy to overlook since the price of the packaging may be relatively low in comparison to the price of the goods, particularly for high-technology items. However, such information can be invaluable. For example, a defendant accused of trafficking 2,000 counterfeit computer chips for $200 each for a total of $400,000 may also have sold 10,000 counterfeit boxes for that same kind of chip at three dollars each for a total of $30,000. Though the $30,000 in box sales may seem like a small part of a $400,000 case, it can provide an important lead concerning the purchaser of the counterfeit boxes. Since the boxes serve no other purpose than to facilitate the trafficking in counterfeit goods, a reasonable inference is that the box purchaser may also be trafficking in the counterfeit chips. Therefore, what was a simple $30,000 worth of boxes could lead to $2 million worth of counterfeit chips.

g. The Probable Sentence or Other Consequences if the Person is Convicted

The consequences that may be imposed if an IP prosecution is successful include imprisonment, restitution, and forfeiture. In *Prosecuting Intellectual Property Crimes*, the sentencing provisions are discussed at § VII.A, whereas restitution (which is generally mandatory in IP cases) is discussed at § VII.B and forfeiture (which is generally available in IP cases) is discussed at § VII.C. The probable sentence is worthy of attention in light of the May 2000 revision to sentencing guideline § 2B5.3 (which is the relevant guideline for most IP crimes) to more accurately reflect the loss caused by IP crime.

Under revised guideline § 2B5.3, the base offense level is 8. This level is increased by reference to the "fraud table" at § 2F1.1 with a calculation where "loss" is based on the "infringement amount." It is important to understand that the "infringement amount" is calculated, in many IP cases, based on the retail value of the *infringed* (legitimate) item multiplied by the number of infringing items. This calculation can profoundly affect the sentence in an IP case.

For example, if a defendant sold, for five dollars each, 100 pirated CDs each containing 20 pirated software programs worth one hundred dollars each, that defendant may have profited only $500. Nevertheless, for sentencing purposes in such a case, the loss would probably be measured by the value of the intellectual property infringed upon by the defendant, which is $2,000 per CD for a total of $200,000.

Since the new sentencing guidelines now recognize in many IP cases that the value of the legitimate property is the proper basis for a loss calculation, prosecutors should be aware of this value in deciding whether to proceed with an IP case. Other important factors that can affect the offense level by 2 points each, are:

1.Whether the offense involved the manufacture, importation, or uploading of infringing items;

2. Whether the offense was not committed for commercial advantage or private financial gain;

3. Whether the offense involved (a) the conscious or reckless risk of serious bodily injury; or (b) possession of a dangerous weapon (including a firearm) in connection with the offense; or

4. Whether the offender took steps to circumvent encryption or other security measures in order to gain initial access to the infringed item.

Other factors that the Sentencing Commission has specifically recognized as possible grounds for an upward departure in an IP case under sentencing guideline § 2B5.3 are:

1. If the reputation of the trademark or copyright owner was substantially harmed by the offense in a way that is not accounted for in the monetary calculation; or

2. If the offense was in connection with or in furtherance of a national or international organized criminal enterprise.

2. Whether the Person is Subject to Prosecution in Another Jurisdiction

The second situation noted by the *U.S. Attorneys' Manual* § 9-27.220 in which the prosecutor may properly decline to take action despite having sufficient admissible evidence occurs when the person is subject to effective prosecution in another jurisdiction. In IP cases, as in other cases, "[a]lthough there may be instances in which a Federal prosecutor may wish to consider deferring to prosecution in another Federal district, in most instances the choice will probably be between Federal prosecution and prosecution by state or local authorities." *U.S. Attorneys' Manual* § 9-27.240 (cmt). In determining whether prosecution should be declined because the person is subject to effective prosecution in another jurisdiction, prosecutors should weigh all relevant considerations, including: (1) the strength of the other jurisdiction's interest in prosecution; (2) [t]he other jurisdiction's ability and willingness to prosecute effectively; and (3) [t]he probable sentence or other consequences if the person is convicted in the other jurisdiction. *U.S. Attorneys' Manual* § 9-27.240. *See United States v. Coffee*, 113 F. Supp.2d 751 (E.D. Pa. 2000) (granting defendants' motion to transfer venue on the basis of the convenience of the parties and witnesses and the interests of justice where the impecunious defendants' home and the alleged criminal operations were in Dayton, Ohio and only five of fifty-seven proposed government witnesses were in Philadelphia, where an undercover operation had purchased counterfeit airplane parts).

IP cases represent a rare species where a prosecutor arguably may not be able to defer to a prosecution in the location of the primary victim. For example, a individual in one state may traffic in counterfeit sports wear bearing the counterfeited mark of a sports team located in a second state, and he might do so without ever physically entering that second state. Because of the defendant's constitutional and statutory right to be tried in the state and district in which their crime was "committed," U.S. Const. art. III § 2 cl. 3; U.S. Const. amend. 6; 18 U.S.C. § 3237, a prosecutor based in that second state—the home state of the victim—arguably may not have proper venue over the counterfeiter unless he or she can show that the "locus delecti" of the counterfeiting took place in the second state. This determination must be made "from the nature of the crime alleged and the location of the act or acts constituting it." *United States v. Rodriguez-Moreno*, 526 U.S. 275, 280 (1999).

Although this subject has not been vigorously litigated in the criminal infringement context, ordinarily the analysis turns on the locations of the actions of the defendant, rather than the district where the harm is felt. For example, in *United States v. DeFreitas*, 92 F. Supp.2d 272, 276-77 (S.D.N.Y. 2000), the district court found New York venue proper in a case under 18 U.S.C. § 2320 where the counterfeit Beanie Babies were shipped from China to Canada, trucked to New York and then to New Jersey because "the very nature of the offense of 'trafficking' contemplates a continuing offense, one which begins with obtaining control over the counterfeit goods, continues with the transport, and ends with the transfer or disposal of such goods." *Cf. United States v. Muench*, 153 F.3d 1298, 1303 (1998) (finding venue for failure to pay child support to be proper in Florida, where victim child lived, even though Texas was where the defendant lived and where his child support checks were due); *United States v. Reed*, 773 F.2d 477, 483 (2d Cir. 1985) (considering factors such as the site of the criminal acts, the elements and nature of the crime, the locus of its effects, and the suitability of the various districts for accurate factfinding and concluding that perjury in one district in a proceeding ancillary to a proceeding in another district may be prosecuted in either). *See generally* Donna A. Balaguer, *Venue*, 30 Am. Crim. L. Rev. 1259 (1993).

Thus, in IP cases, it is common that the federal prosecutor will be called upon to vindicate the rights of a victim IP holder based in another district, another state, or even another country. Prosecutors should therefore be cognizant that the defendant may not be subject to prosecution in the victim's district, state or nation. Federal prosecutors should also recognize that local or state authorities may not have a great interest in punishing violations of the rights of out-of-state victim IP holders. By contrast, ensuring uniform

and reliable national enforcement of the IP laws is an important goal of federal law enforcement.

This goal takes on added significance for federal prosecutors when the victim is based in a foreign country because of the importance of IP in modern international trade. With consistent enforcement of IP rights, America will continue to set an example of vigorous IP rights enforcement and to be perceived as hospitable to foreign firms that would register their IP and engage in business here.

Local and state authorities may also believe that since many IP rights are conferred by the federal government, they do not have the ability to prosecute any IP crimes. There is a provision for federal preemption for copyright infringement, 17 U.S.C. § 301, although this preemption permits prosecution for other kinds of crime.

Even if the local or state authorities express a strong interest in prosecution, they may not have the ability or willingness to prosecute the case effectively. IP cases may not be a priority for some state or local authorities. They may have limited resources to devote to IP cases. For example, a particular office may not have space to store the large inventory seized from the warehouse of a counterfeiter. Some state or local authorities may not be interested in vindicating the IP rights of a distant victim. For a further discussion of state and local authority to prosecute IP crimes and a listing of state criminal IP statutes, see *Prosecuting Intellectual Property Crimes* § VI.A.2 & App. D (2001).

3. The Adequacy of a Noncriminal Alternative in an IP Case

Prosecutors may consider the adequacy of noncriminal alternatives when addressing an IP case. Some civil remedies, including *ex parte* seizure of a defendant's infringing products and punitive damages, may be available for certain violations of copyright and trademark rights. 15 U.S.C. § 1116(d) (trademark remedies); 17 U.S.C. §§ 502-505 (copyright remedies). Also, for importers of trademark-infringing merchandise, the Customs Service may assess civil penalties not greater than the value that the merchandise would have were it genuine, according to the manufacturer's suggested retail price for first offenders, and not greater than twice that value for repeat offenders. These civil fines may be imposed in the U.S. Custom Service's discretion, in addition to any other civil or criminal penalty or other remedy authorized by law. 19 U.S.C. § 1526(f). The availability and adequacy of these remedies should be carefully considered when evaluating an IP case.

Yet civil remedies may be futile under various circumstances. For example, IP crimes are unusual because they generally are committed without the victim's knowledge, even after the fact. The victim usually has no direct relationship with the infringer—before, during, or after the commission of the crime. If a victim is unaware of a violation by a particular defendant, civil remedies generally will be unavailing. Furthermore, without criminal sanction, infringers or counterfeiters might treat the rare case of the victim's civil enforcement of its rights as a cost of doing business.

Another important factor to consider when contemplating civil remedies is that infringers may be judgment proof. In most cases, the infringer traffics in counterfeit items worth far less than the authentic ones. By the time law enforcement identifies the unlawful activity, the value of the infringing items that the defendant has distributed often far exceeds the funds to which the defendant has access. This phenomenon is particularly common in software infringement cases, since an infringer can reproduce large numbers of high quality copies with only minimal investment. In Internet and computer bulletin board cases, a relatively modest expenditure in a personal computer and a modem can result in the reproduction and distribution of hundreds or even thousands of exact duplications of copyrighted works. In such instances, a criminal sanction may be the only meaningful deterrent.

There are a number of other circumstances where existing civil remedies may simply be an insufficient deterrent. For example, there may be cases where there have been prior unsuccessful efforts by a victim to enforce IP rights against the defendant or the existence of circumstances preventing such efforts. Criminal charges may

also be necessary if counterfeiting continues despite the entry of a permanent injunction or consent decree in a civil case. As these scenarios illustrate, there are numerous situations where civil remedies may not deter the infringement, particularly where the defendant regards civil penalties as a cost of doing business. Another option to keep in mind in civil cases where there is a "repeat infringer" is that the existence of a civil order may provide a basis for a petition to the court for contempt.

Finally, civil remedies may not fully capture the wrongfulness of the defendant's criminal conduct. Counterfeiting or infringement of IP threatens the very integrity of the federal IP system, just as counterfeiting of currency jeopardizes the currency system. A meaningful threat of criminal prosecution is necessary to safeguard the public's confidence in IP.

Conclusion

Because defendants in IP cases can have several victims, including the IP holders, society at large, and the recipients of the infringing goods or works, and because reliable enforcement of federally created IP rights is so important to the growing information economy, federal prosecutors should carefully consider whether to prosecute an IP case. Since the enactment in May 2000 of the new sentencing guideline that more accurately reflects the loss caused by IP crime, the punishment that can arise from a conviction is now more appropriate to the crime. Prosecutors should be aware of these special characteristics of IP cases when evaluating them against traditional principles and exercising their prosecutorial discretion. Further guidance is available from the recently published manual, *Prosecuting Intellectual Property Crimes* (2001), or from the IP Team at the Computer Crime and Intellectual Property Section (CCIPS) at (202) 514-1026. ˜

ABOUT THE AUTHOR

‘ **David Goldstone** has been a Trial Attorney in the Computer Crime and Intellectual Property Section for four years. He is the Team Leader for the Intellectual Property Team, and the primary author and editor of *Prosecuting Intellectual Property Crimes* (2001). Mr. Goldstone has been an instructor at the National Advocacy Center and is an adjunct professor of cyberspace law at the law schools of Georgetown University and George Washington University.a

Recognizing and Meeting Title III Concerns in Computer Investigations

Robert Strang
Assistant United States Attorney
Southern District of New York

The dramatic increase in crimes involving the Internet, and computer crimes more generally, is well documented. The "2000 CSI/FBI Computer Crime and Security Survey" documented that 90% of the 643 respondents (primarily large U.S. corporations and government agencies) detected computer security breaches within the last twelve months, totaling hundreds of millions of dollars in losses. In light of the increased criminal opportunities created by the ever-growing reliance on, and growing interconnectedness between network computers, there can be no doubt that experienced and sophisticated computer criminals pose a substantial challenge to law enforcement.

There has also been a corresponding increase in the difficulty in catching computer criminals. There are a number of reasons why this is so. The anonymity provided by computer communications has long been recognized as one of the major

attractions to would-be computer criminal subjects. This difficulty has been heightened by the use and availability of so-called "anonymizers", services that repackage electronic mail and thereby diminish the ability to trace it. In addition, many victims and Internet Service Providers (ISPs) fail to record, or preserve for a sufficient length of time, historical logs and other records that might otherwise lead to the identification of subjects engaged in wrongdoing. Furthermore, the practice of jumping from compromised network to compromised network, including networks with servers located outside of the United States, can also make tracing the communications back to the initial subject extremely difficult. This is especially true where subjects have made efforts to cover their tracks or where proof of criminal activity, or even their fleeting presence, is lost before it can be secured. Finally, victims may be unaware of criminal activity on their network or, if aware, slow or unwilling to report it due to competitive reasons. For these and other reasons, there are many computer crimes where it will be impossible for law enforcement to identify the perpetrators involved. Therefore, exclusive reliance on historical investigations will allow criminal activity carried out by more experienced and skillful criminals to go undetected and/or unpunished.

Issues Raised by Proactive Investigations

As a result of these limitations, law enforcement is increasingly turning to proactive investigations where undercover agents seek out the individuals who are already engaging in computer crimes — attempting to record, in real-time, computer criminals while they are involved in the criminal act. The proactive approach bypasses some of the investigatory hurdles of anonymity, lack of records, and under-reporting inherent in computer cases. It also has the added benefit of potentially stopping the criminal before the damage is done. Use of real-time monitoring of criminal activity is even advantageous in some historical investigations where a subject returns to, or passes through the same victim's network. As criminals are increasingly adept at avoiding leaving an historic trail, such investigations are the next logical step for law enforcement (and one that is increasingly being taken).

Such undercover operations and recording are also feasible. The very expectation of anonymity that benefits criminals also helps law enforcement undercover agents enter this world without being scrutinized, as long as they can talk the talk. Agents can even use other undercover identities to vouch for themselves. From a technical perspective, so-called "sniffer" computer programs that are capable of recording all keystroke activity on a particular computer network are a well-known and widely available tool for system administrators, hackers, and law enforcement alike.

These types of investigatory techniques often raise legal issues. One of the major issues raised by real-time monitoring is compliance with federal wiretapping statutes. This article focuses on the ability to legally and contemporaneously record and identify subjects, and to develop admissible evidence which is central to a successful investigation. Agents and other investigators, some with only limited experience in this area may turn to prosecutors with questions regarding what they can and cannot do in their efforts to use real-time monitoring of criminals during the course of undercover operations. It is critical for prosecutors to be able to identify potential legal issues relating to such recordings by agents, in advance, before problems arise.

Since the current legal road map is largely without judicial markers, it is important to address some of the potential issues raised by the application of the privacy laws to real-time monitoring, as well as some of the statutory exceptions that may permit monitoring to take place absent a court order.

Application of Title III to "Electronic Communications"

In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA"), which, among others things, extended the prohibitions contained in Title III of the Omnibus Crime and Control and Safe Streets Act of 1968 (the "Wiretap Act"), 18 U.S.C. §§ 2510-2521, to electronic communications that are intercepted

contemporaneously with their transmission—that is electronic communications that are in transit between machines and which contain no aural (human voice) component. Thus, communications involving computers, faxes, and pagers (other than "tone-only" pagers) all enjoy the broad protections provided by Title III *unless* one or more of the statutory exceptions to Title III applies. In the computer context, both the government and third parties are prohibited from installing "sniffer" computer software, such as the FBI's Carnivore program, to record keystroke and computer traffic of a specific target unless one of the exceptions is present.

Where the government is seeking to intercept and monitor all electronic communications originating from a target's home or through the e-mail account at the target's ISP, the application of Title III differs little from its historical application to telephone wiretaps. The issues agents and prosecutors are likely to encounter are typically technical, not legal. This is particularly true when law enforcement is dealing with ISPs who may have little or no experience in providing Title III assistance to law enforcement, have technical or manpower difficulties in providing access to the subject's accounts, or show an overall reluctance in working with law enforcement.

Sometimes, however, the potential effect of Title III's restrictions on computer law enforcement can be unexpected. For example, if a hacker breaks into a victim's computer, engages in criminal activity, and uses it to store credit card numbers, common sense would suggest the subject hacker enjoys no reasonable expectation of privacy. Perversely, however, the subject hacker's communications may enjoy statutory protection under Title III, and thus any interception of that illegal activity by a private party (including the victim) or law enforcement must fall within one of the statutory exceptions in order to monitor without a court order. In the above example, the victim's consent is likely to be sufficient to fall within one of Title III's statutory exceptions.

This example, however, becomes more difficult if the subject hacker simply uses the victim's computer as a jump point from which to illegally hop to new downstream victims or to communicate with the hacker's confederates, as is frequently the case. Does a victim have a right to monitor communications that are being made by a subject hacker who is trespassing on their computer, and is no longer seeking to damage it, but rather is passing through on his or her way to commit more mischief? Does the government enjoy the same rights to monitor that communication as the victim? How, if at all, does the analysis change when the government is the primary victim of the hacking activity?

The analysis of these scenarios is currently dependent on how courts interpret the breadth of existing statutory exceptions to Title III that were written to address the interception of simple, two-way telephone conversations. Thus, under current law, a hacker, a trespasser on another party's computer network, an intruder who enjoys no expectation of privacy, may nevertheless receive certain statutory protections under Title III. Prosecutors must therefore consider whether the statutory exceptions to Title III permit any proposed monitoring. The following are three statutory exceptions that appear to offer potential alternatives to the administrative and judicial burdens involved in seeking court-ordered monitoring under Title III.

Consent of a Party "Acting Under Color of Law"

The most commonly used exception to Title III's requirements permits "a person acting under color of law" to intercept an "electronic communication" where "such person is a party to the communication, or one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(c).

While there are not many judicial decisions in this area, two circuits appear to recognize that the owner of a computer may be considered a "party to the communication" and thus can consent to the government monitoring electronic communications between that computer and a hacker. *See United States* v. *Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993); *United States* v. *Seidlitz*, 589 F.2d 152, 158 (4th Cir. 1978). Thus, this exception appears to permit a victim to monitor and to authorize the government to

monitor, hacking activity directly with his or her computer.

By contrast, if the communication merely passes through a victim's computer, a court may consider it a strain to conclude that the victim computer is a "party" to the communication. Technically, the victim's computer is receiving electronic communications and passing them on to downstream victims and/or confederates of the subject hacker. The literal possibility of monitoring this downstream traffic is present, as all the data streams through the victim's computer, but is the victim a "party to the communication" if the communications are simply passing through its system? A court may conclude that the owner is not a "party" capable of giving consent to key stroke monitoring given its pass through role.

This is more than a metaphysical concern. Hackers regularly seek to pass through the computers of victims they have previously hacked to: (1) cover their trail when they arrive at their next victim or victims; (2) continue to make use of favorable features of a compromised network such as storage space, bandwidth, and processing speed; (3) return to hacking tools they have left there for safekeeping; or (4) simply as a pattern of passing through old conquests to make sure their previous exploits have not been detected. This situation can arise even when a government computer is the initial victim. From there, the subject may hop (typically telnet) to the next network without taking the trouble of backing out of the hacked system. It is possible that the downstream network may not even be a true victim, but rather may belong to a system friendly to the subject hacker. In any event, the statutory exception requires that this new victim give "prior consent" to the monitoring, which will be almost an impossibility in the short term where the victim or victims typically cannot be known in advance.

Consent of a Party "Not Acting Under Color of Law"

Title III also permits "a person not acting under color of law" to intercept an "electronic communication" where "such person is a party to the communication, or one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(d).

In addition to permitting a victim to monitor communications to which he or she is a party before law enforcement gets involved, this exception provides a very powerful tool to law enforcement: obtaining the implied consent of the subject hacker himself or herself through computer "banners."

Computer networks frequently make use of computer banners that appear whenever a person logs onto the network. Each of us, for example, passes through such a banner each day when we log onto the Department of Justice's computer network. A banner is nothing more than a program that is installed to appear whenever a user attempts to enter a network from a designated point of entry known as a "port." Banners vary substantially in wording, but they usually inform the user that: (1) the user is on a private network; and (2) by proceeding, the user is consenting to all forms of monitoring. Government networks already employ such broad-based banners, and we encourage private industry to follow suit. Businesses are often amenable to doing so, although often for non-law enforcement purposes, such as the monitoring of their employees' use of the Internet.

Thus, the subject hacker gives implied consent to monitoring whenever he or she passes through a properly worded banner. A properly worded banner should also result in implied consent by the subject hacker to the monitoring of all downstream activities, thus alleviating Title III concerns in much the same way as telephone monitoring of inmates, based on implied consent, has been upheld by the courts.

Due to their pervasiveness, the presence of banners is unlikely to deter or arouse suspicion in a subject who has already decided to enter a network illegally. In the case where a private network failed to have a sufficiently broad banner to permit monitoring, a later attempt to add a banner between visits may cause suspicion on the part of the hacker. Even in this situation, however, the very nature of the hacking experience frequently involves the constant cat and mouse game between network system administrators,

seeking to remove hackers from their systems by terminating a compromised account and/or by "patching" the vulnerability that permitted the hackers to illegally enter the network, and the hackers attempting to return to the system and overcome and disable its security features. Thus, the addition of a new banner may not concern a dedicated hacker. The subject hacker may not be aware that Title III may prevent law enforcement from monitoring all of the intruder's activities while he or she is connected to the compromised computer network.

Finally, there are technical limitations to the use of banners. Computer systems are designed to have hundreds of ports for different types of uses such as electronic mail, remote log-in, or telnet. Most of these ports are not in use and remain closed, and can only be opened by a system administrator, or by a hacker who has illegally obtained the same privileges as a system administrator. Due to the technical nature of these ports, which goes beyond the scope of this article, it is not possible to install a banner or other message on a certain percentage of the ports. It is possible for a determined hacker to gain the same privileges (known as "superuser" or "root" status) on a network and open one or more of these ports, perhaps to serve as a future "back door" means of entry. Having once been given notice that the subject has given implied consent to monitoring by making use of a network, however, that consent should be valid for future use whether entry was made through a bannered or a non-bannered port. The only question this possibility raises is whether an affiliated or unaffiliated hacker might use one of these non-bannered ports for entry, and never pass through a banner.

Protection of the Rights and Property of the Provider

Title III also permits providers of a communication service, including an electronic communication service, the right to intercept communications as a "necessary incident to the rendition of his service" or to protect "the rights or property of the provider of that service." 18 U.S.C. § 2511(2)(a)(i).

This exception permits a private party to monitor activities on its system to prevent misuse of the system through damage, fraud, or theft of services. Since computer hacking often involves damage or disabling of a network's computer security system, as well as theft of the network's service, this exception permits a system administrator to monitor the activities of a hacker while on the network.

This exception to Title III has some significant limitations. One important limitation is that the monitoring must be reasonably connected to the protection of the provider's service, and not as a pretext to engage in unrelated monitoring. While no court has explored what this limitation means in the computer context, by way of analogy, one court has held that a telephone company may not monitor all the conversations of a user of an illegal clone phone unrelated to the protection of its service. *See McClelland* v. *McGrath*, 31 F. Supp.2d 616 (N.D. Ill. 1998).

Furthermore, the right to monitor is justified by the right to protect one's own system from harm. An ISP, for example, may not be able to monitor the activities of one of its customers under this exception for allegedly engaging in hacking activities on other networks. This limitation also makes it harder for a network administrator to justify the monitoring of hacking activities of a subject who has jumped to a new downstream victim. This potential limitation is unfortunate as it becomes more applicable precisely when the consent of a "party to the communication" is also at its weakest.

Another important limitation of this exception is that it does not permit a private provider of the communication service to authorize the government to conduct the monitoring; the monitoring must be done by the provider itself. Thus, where a provider lacks the technical or financial resources, or desire to engage in monitoring itself, it may be difficult for the government to step in to assist. Similarly, in situations where the government becomes aware that an ISP or network system administrator is monitoring illegal activity in order to protect its "rights and property," the government should be careful not to direct or participate in the monitoring, or cause it to be continued, because the provider may be deemed an agent of the

government, and the exception may not apply. *Compare United States* v. *Pervaz*, 118 F.3d 1 (1st Cir. 1997), with *McClelland*, *infra*.

Even with these limitations, the provider exception can be very useful, particularly when a system administrator aggressively chooses to investigate hacking activity, or when the victim computer network is owned by the government. The technical gap in the use of implied consent described above, the inability to place consent banners on certain ports, can be filled by the use of the provider exception to monitor computer intrusions coming through these ports.

Conclusion

While Title III concerns are only one of the potential issues raised by proactive investigations in the computer context (others may include entrapment or even third-party liability), they are certainly among the most important. When all else fails, the prosecutor can always seek a Title III interception order. While this requires both departmental and judicial approval, there are a few aspects of obtaining such a "datatap" order that may make it less of a burden than obtaining a traditional telephone wiretap order. First, with respect to the interception of electronic communications, law enforcement is not limitedto predicate offenses, but rather may seek it for any federal felony (note that some forms of hacking may constitute only a misdemeanor). *See* 18 U.S.C. § 2516(3). Second, with respect to the recording on or through a victim computer, the actual hacking activities typically constitute a federal felony, thus meeting the probable cause standards for seeking the authorization will be simple. *See* 18 U.S.C. § 2518(3)(a). Third, the method of recording the results of the datatap are not difficult; the information can be obtained using specialized software or commercially available sniffer programs. Finally, minimization presents far less of a problem than it does for the execution of a traditional wiretap. *See* 18 U.S.C. § 2518(5). The burdens encountered and time lost in seeking Title III authorization makes the proper use of the exceptions discussed in this article extremely useful tools in investigating criminal activity. With the aid of proper monitoring, as well as the use of the many tools to obtain historical activities of subject hackers, law enforcement can overcome the potential anonymity provided by a computer, and identify and prosecute those criminals who abuse it to violate the law.

For more information on how Title III applies to the Internet, see Chapter 4 of the Computer Crime and Intellectual Property Section's new manual "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Criminal Investigations. It is available at www.cybercrime.gov/searchmanual.htm" ~

ABOUT THE AUTHOR

‘ **Robert Strang** has been an Assistant United States Attorney for the Southern District of New York since 1997, where he currently serves as Computer Telecommunications Coordinator.a

Identity Theft: The Crime of the New Millennium

Sean B. Hoar
Assistant United States Attorney
District of Oregon

The Nature of the Problem

Identity theft has been referred to by some as the crime of the new millennium. It can be accomplished anonymously, easily, with a variety of means, and the impact upon the victim can be devastating. Identity theft is simply the theft of identity information such as a name, date of birth, Social Security number (SSN), or a credit card number. The mundane activities of a typical consumer during the course of a regular day may provide tremendous opportunities for an identity thief: purchasing gasoline, meals, clothes, or tickets to an athletic event; renting a car, a video, or home-improvement tools; purchasing gifts or trading stock on-line; receiving mail; or taking out the garbage or recycling. Any activity in which identity information is shared or made available to others creates an opportunity for identity theft.

It is estimated that identity theft has become the fastest-growing financial crime in America and perhaps the fastest-growing crime of any kind in our society. *Identity Theft: Is There Another You?: Joint hearing before the House Subcomms. on Telecommunications, Trade and Consumer Protection, and on Finance and Hazardous Materials, of the Comm. on Commerce*, 106th Cong. 16 (1999) (testimony of Rep. John B. Shadegg). The illegal use of identity information has increased exponentially in recent years. In fiscal year 1999 alone, the Social Security Administration (SSA) Office of Inspector General (OIG) Fraud Hotline received approximately 62,000 allegations involving SSN misuse. The widespread use of SSNs as identifiers has reduced their security and increased the likelihood that they will be the object of identity theft. The expansion and popularity of the Internet to effect commercial transactions has increased the opportunities to commit crimes involving identity theft. The expansion and popularity of the Internet to post official information for the benefit of citizens and customers has also increased opportunities to obtain SSNs for illegal purposes.

On May 31, 1998, in support of the Identity Theft and Assumption Deterrence Act, the General Accounting Office (GAO) released a briefing report on issues relating to identity fraud entitled "Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited". The report found that methods used to obtain identity information ranged from basic street theft to sophisticated, organized crime schemes involving the use of computerized databases or the bribing of employees with access to personal information on customer or personnel records. The report also found the following: In 1995, 93 percent of arrests made by the U.S. Secret Service Financial Crimes Division involved identity theft. In 1996 and 1997, 94 percent of financial crimes arrests involved identity theft. The Secret Service stated that actual losses to individuals and financial institutions which the Secret Service had tracked involving identity fraud totaled $442 million in fiscal year 1995, $450 million in fiscal year 1996, and $745 million in fiscal year 1997. The SSA OIG stated that SSN misuse in connection with program fraud increased from 305 in fiscal year 1996 to 1,153 in fiscal year 1997. Postal Inspection investigations showed that identity fraud was perpetrated by organized crime syndicates, especially to support drug trafficking, and had a nationwide scope. Trans Union Corporation, one of the three major national credit bureaus, stated that two-thirds of its consumer inquiries to its fraud victim department involved identity fraud. Such inquiries had increased from an average of less than 3,000 a month in 1992 to over 43,000 a month in 1997. VISA U.S.A., Inc., and MasterCard International, Inc. both stated that overall fraud losses from their member banks were in the hundreds of millions of dollars

annually. MasterCard stated that dollar losses relating to identity fraud represented about 96 percent of its member banks' overall fraud losses of $407 million in 1997.

Victims of identity theft often do not realize they have become victims until they attempt to obtain financing on a home or a vehicle. Only then, when the lender tells them that their credit history makes them ineligible for a loan, do they realize something is terribly wrong. When they review their credit report, they first become aware of credit cards for which they have never applied, bills long overdue, unfamiliar billing addresses, and inquiries from unfamiliar creditors. Even if they are able to identify the culprit, it may take months or years, tremendous emotional anguish, many lost financial opportunities, and large legal fees, to clear up their credit history.

How Does Identity Theft Occur?

Identity theft occurs in many ways, ranging from careless sharing of personal information, to intentional theft of purses, wallets, mail, or digital information. In public places, for example, thieves engage in "shoulder surfing" **n** watching you from a nearby location as you punch in your telephone calling card number or credit card number **n** or listen in on your conversation if you give your credit card number over the telephone. Inside your home, thieves may obtain information from your personal computer while you are on-line and they are anonymously sitting in the comfort of their own home. Outside your home, thieves steal your mail, garbage, or recycling. Outside medical facilities or businesses, thieves engage in "dumpster diving" **n** going through garbage cans, large dumpsters, or recycling bins **n** to obtain identity information which includes credit or debit card receipts, bank statements, medical records like prescription labels, or other records that bear your name, address, or telephone number.

In a recent case in the District of Oregon, a ring of thieves obtained identity information by stealing mail, garbage, and recycling material, by breaking into cars, and by hacking into web sites and personal computers. The thieves traded the stolen information for methamphetamine, cellular telephones, or other favors. Before they were arrested, they had gained access to an estimated 400 credit card accounts and had made an estimated $400,000 in purchases on those fraudulently obtained accounts. One aspect of the case involved the theft of preapproved credit card solicitations, activating the cards, and having them sent to drop boxes or third-party addresses. Another scam involved taking names, dates of birth, and SSNs from discarded medical, insurance, or tax information and obtaining credit cards at various sites on the Internet. The thieves found most credit card companies to be unwitting allies. One of the thieves boasted about successfully persuading a bank to grant a higher credit limit on a fraudulently obtained credit card account. Another aspect of the case involved the use of a software application to hack into commercial web sites or personal computers and mirror keystrokes to capture credit card account information. Two of the offenders were prosecuted federally for conspiracy to commit computer fraud and mail theft under 18 U.S.C. §§ 1030(a)(4), 371and 1708, and consented to the forfeiture of computer equipment obtained as a result of the fraud-related activity pursuant to 18 U.S.C. § 982(a)(2)(B). One defendant was sentenced to serve a forty-one month term of imprisonment and pay $70,025.98 in restitution. *United States v. Steven Collis Massey*, CR 99-60116-01-AA (D.Or. 1999). The other defendant was sentenced to serve a fifteen month term of imprisonment and pay $52,379.03 in restitution. *United States v. Kari Bahati Melton*, CR 99-60118-01-AA (D.Or. 1999).

How Can Identity Theft Be Investigated and Prosecuted?

The investigation of identity theft is labor intensive and individual cases are usually considered to be too small for federal prosecution. Perpetrators usually victimize multiple victims in multiple jurisdictions. Victims often do not realize they have been victimized until weeks or months after the crime has been committed, and can provide little assistance to law enforcement. In short, identity theft has become the fastest-growing financial crime in America and perhaps the fastest-growing crime of any kind in our society, because offenders are seldom held accountable. Consequently, it has become a priority for the Departments of Justice and

Treasury and the Federal Trade Commission (FTC) to pursue effective means of prevention, investigation, and prosecution of identity theft offenses. Toward that end, workshops were recently held for the purpose of identifying the best practices to combat identity theft, including remediation, prevention, and law enforcement strategies. Workshop participants included prevention specialists, federal agency representatives, state and federal investigators, and state and federal prosecutors.

The experience of workshop participants is that law enforcement agencies at all levels, federal and non-federal, must work together investigating identity theft. Multi-agency task forces have proven successful in investigating and prosecuting identity theft. By utilizing task forces, member agencies pool scarce resources to investigate and prosecute identity theft offenses, and provide prevention training. Workshop participants also indicated that outreach to private industry is necessary as a prevention strategy, and it facilitates the identification of offenders.

Identity theft cases involving large numbers of victims present unique challenges. One challenge is communication with victims. Communication is necessary to obtain fundamental investigative information, including loss and restitution information. In complex cases, it is imperative to devise a system for communication with the victims at the outset of the case. The AUSA should work with victim/witness units to identify the best communication system for the case. The AUSA should also work with the system administrator to develop a link from the district's web site for on-line communication with victims. The link can provide access to a data base into which victims can enter case-related information. The link can also be used to provide updates on the status of the case. Notification to the victims regarding their use of the web site can be provided through a form letter accompanying an investigative survey which must be completed, in any event, to obtain loss and restitution information.

1. Federal Criminal Laws

There are a number of federal laws applicable to identity theft, some of which may be used for prosecution of identity theft offenses, and some of which exist to assist victims in repairing their credit history. The primary identity theft statute is 18 U.S.C. § 1028(a)(7) and was enacted on October 30, 1998, as part of the Identity Theft and Assumption Deterrence Act (Identity Theft Act). The Identity Theft Act was needed because 18 U.S.C. § 1028 previously addressed only the fraudulent creation, use, or transfer of identification *documents*, and not the theft or criminal use of the underlying personal *information*. The Identity Theft Act added § 1028(a)(7) which criminalizes fraud in connection with the unlawful theft and misuse of personal identifying information, regardless of whether the information appears or is used in documents. Section 1028(a)(7) provides that it is unlawful for anyone who:

> knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law. . . .

The Identity Theft Act amended the penalty provisions of § 1028(b) by extending its coverage to offenses under the new § 1028(a)(7) and applying more stringent penalties for identity thefts involving property of value. Section 1028(b)(1)(D) provides for a term of imprisonment of not more than fifteen years when an individual commits an offense that involves the transfer or use of one or more means of identification if, as a result of the offense, anything of value aggregating $1,000 or more during any one year period is obtained. Otherwise, § 1028(b)(2)(B) provides for imprisonment of not more than three years. The Identity Theft Act added § 1028(f) which provides that attempts or conspiracies to violate § 1028 are subject to the same penalties as those prescribed for substantive offenses under § 1028.

The Identity Theft Act amended § 1028(b)(3) to provide that if the offense is committed to facilitate a drug trafficking crime, or in connection with a crime of violence, or is committed by a

person previously convicted of identity theft, the individual is subject to a term of imprisonment of not more than twenty years. The Identity Theft Act also added § 1028(b)(5) which provides for the forfeiture of any personal property used or intended to be used to commit the offense.

Section 1028(d)(3) defines "means of identification", as used in § 1028(a)(7), to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual." It covers several specific examples, such as name, social security number, date of birth, government issued driver's license and other numbers; unique biometric data, such as fingerprints, voice print, retina or iris image, or other physical representation; unique electronic identification number; and telecommunication identifying information or access device.

Section 1028(d)(1) modifies the definition of "document-making implement" to include computers and software specifically configured or primarily used for making identity documents. The Identity Theft Act is intended to cover a variety of individual identification information that may be developed in the future and utilized to commit identity theft crimes.

The Identity Theft Act also directed the United States Sentencing Commission to review and amend the Sentencing Guidelines to provide appropriate penalties for each offense under Section 1028. The Sentencing Commission responded to this directive by adding U.S.S.G. § 2F1.1(b)(5) which provides the following:

> (5) If the offense involved –
>
> (A) the possession or use of any device-making equipment;
>
> • the production or trafficking of any unauthorized access device or counterfeit access device; or
>
> • (i) the unauthorized transfer or use of any means of identification unlawfully to produce or obtain any other means of identification; or (ii) the possession of [five] or more means of identification that unlawfully were produced from another means of identification or obtained by the use of another means of identification,
>
> increase by 2 levels. If the resulting offense level is less than level 12, increase to level 12.

These new guidelines take into consideration the fact that identity theft is a serious offense, whether or not certain monetary thresholds are met. For most fraud offenses, the loss would have to be more than $70,000.00 for the resulting offense level to be level 12. U.S.S.G. § 2F1.1(b)(1)(G). In providing for a base offense level of 12 for identity theft, the Sentencing Commission acknowledged that the economic harm from identity theft is difficult to quantify, and that whatever the identifiable loss, offenders should be held accountable. Identity theft offenses will usually merit a two-level increase because they often involve more than minimal planning or a scheme to defraud more than one victim. U.S.S.G. § 2F1.1(b)(2). Identity theft offenses may also provide for two to four-level upward organizational role adjustments when multiple defendants are involved. U.S.S.G. § 3B1.1

The Identity Theft Act also directed the FTC to establish a procedure to log in and acknowledge receipt of complaints from victims of identity theft, to provide educational materials to these victims, and to refer the complaints to appropriate entities. The FTC has responded to this directive by developing a web site, great educational materials, a hotline for complaints, and a central database for information. The web site can be found at www.consumer.gov/idtheft. The hotline is 1-877-ID THEFT. Identity theft complaints are entered into Consumer Sentinel, a secure, on-line database available to law enforcement. The FTC has become a primary referral point for victims of identity theft, and a tremendous resource for these victims and law enforcement.

2. Other Federal Offenses

Identity theft is often committed to facilitate other crimes, although it is frequently the primary goal of the offender. Schemes to commit identity theft may involve a number of other statutes

including identification fraud (18 U.S.C. § 1028(a)(1) - (6)), credit card fraud (18 U.S.C. § 1029), computer fraud (18 U.S.C.§ 1030), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), financial institution fraud (18 U.S.C. § 1344), mail theft (18 U.S.C. § 1708), and immigration document fraud (18 U.S.C. § 1546). For example, computer fraud may be facilitated by the theft of identity information when stolen identity is used to fraudulently obtain credit on the Internet. Computer fraud may also be the primary vehicle to obtain identity information when the offender obtains unauthorized access to another computer or web site to obtain such information. These acts might result in the offender being charged with both identity theft under 18 U.S.C. § 1028(a)(7) and computer fraud under 18 U.S.C. § 1030(a)(4). Regarding computer fraud, note that U.S.S.G. § 2F1.1(c)(1) provides a minimum guideline sentence, notwithstanding any other adjustment, of a six month term of imprisonment if a defendant is convicted of computer fraud under 18 U.S.C. § 1030(a)(4).

Several examples of how identity theft schemes may involve other statutes may be helpful. These include the case of an offender who fraudulently obtains identity information by posing as an employer in correspondence with a credit bureau. This offender might appropriately be charged with both identity theft under 18 U.S.C. § 1028(a)(7) and mail fraud under 18 U.S.C. § 1341. An offender who steals mail thereby obtaining identity information might appropriately be charged with identity theft under 18 U.S.C. § 1028(a)(7) and mail theft under 18 U.S.C. § 1708. The offender who fraudulently poses as a telemarketer thereby obtaining identity information might appropriately be charged with both identity theft under 18 U.S.C. § 1028(a)(7) and wire fraud under 18 U.S.C. § 1343.

3. Recent Federal Cases

A number of cases have recently been prosecuted under 18 U.S.C. § 1028(a)(7) including the following:

In the Central District of California, a man was sentenced to a twenty-seven month term of imprisonment for obtaining private bank account information about an insurance company's policyholders, while serving as a temporary employee of the company. Thereafter he used that information to deposit over $764,000 in counterfeit bank drafts and withdraw funds from accounts of policyholders. *United States v. Anthony Jerome Johnson*, CR 99-926 (C.D.Ca. Jan. 31, 2000).

In the District of Delaware, one defendant was sentenced to a thirty-three month term of imprisonment and $160,910.87 in restitution, and another defendant to a forty-one month term of imprisonment and $126,298.79 in restitution for obtaining names and SSNs of high-ranking military officers from an Internet web site and using them to apply on-line for credit cards and bank and corporate credit in the officers' names. *United States v. Lamar Christian*, CR 00-3-1 (D. Del. Aug. 9, 2000); *United States v. Ronald Nevison Stevens*, CR 00-3-2 (D.Del. Aug. 9, 2000).

In the District of Oregon, seven defendants have been sentenced to imprisonment for their roles in a heroin/methamphetamine trafficking organization, which included entering the United States illegally from Mexico and obtaining SSNs of other persons. The SSNs were then used to obtain temporary employment and identification documents in order to facilitate the distribution of heroin and methamphetamine. In obtaining employment, the defendants used false alien registration receipt cards, in addition to the fraudulently obtained SSNs, which provided employers enough documentation to complete employment verification forms. Some of the defendants also used the fraudulently obtained SSNs to obtain earned income credits on tax returns fraudulently filed with the Internal Revenue Service. Some relatives of narcotics traffickers were arrested in possession of false documents and were charged with possessing false alien registration receipt cards and with using the fraudulently obtained SSNs to obtain employment. A total of twenty-seven defendants have been convicted in the case to date, fifteen federally and twelve at the state level. *United States v. Jose Manuel Acevez Diaz*, CR 00-60038-01-HO (D.Or. Aug. 10, 2000); *United States v. Pedro Amaral Avila*, CR 00-60044-01-HO (D.Or. Nov. 7, 2000); *United States*

v. Jose Arevalo Sanchez; CR 00-60040-01-HO (D.Or. Nov. 21, 2000); *United States v. Maria Mersedes Calderon*, CR 00-60046-01-HO (D.Or. May 10, 2000); *United States v. Victor Manuel Carrillo*, CR 00-60045-01-HO (D.Or. Oct. 24, 2000); *United States v. Alfonso Flores Ramirez*, CR 00-60043-01-HO (D.Or. Aug. 30, 2000); *United States v. Cleotilde Fregoso Rios*, CR 00-60035-01-HO (D.Or. Nov. 7, 2000); *United States v. Javier Hernandez Lopez*, CR 00-60038-01-HO (D.Or. Aug. 10, 2000); *United States v. Ranulfo Salgado*, CR 00-60039-01-HO (D.Or. Jan. 18, 2001); *United States v. Angel Sanchez*, CR 00-60080-01-HO (D.Or. Aug. 31, 2000); *United States v. Cresencio Sanchez*, CR 00-60143-01-HO (D.Or. Dec. 13, 2000); *United States v. Piedad Sanchez*, CR 00-60131-01-HO (D.Or. Jan. 9, 2001); *United States v. Noel Sanchez Gomez*, CR 00-60034-01-HO (D.Or. Dec. 12, 2000); *United States v. Kelly Wayne Talbot*, CR 00-60081-01-HO (D.Or. Dec. 31, 2000); *United States v. Jose Venegas Guerrero*, CR 00-60037-01-HO (D.Or. Nov. 21, 2000); *State of Oregon v. Fred Harold Davis*, Case No. 006276FE (Jackson County Dec. 13, 2000); *State of Oregon v. Pablo Macias Ponce*, Case No. 004317MI (Jackson County Sept. 13, 2000); *State of Oregon v. Raul Navarro Guiterrez*, Case No. 005257FE (Jackson County Nov. 8, 2000); *State of Oregon v. Miranda Mae Byrne*, Case No. 004363FE (Jackson County Jan. 9, 2001); *State of Oregon v. James Tracy Campbell*, Case No. 002376FE (Jackson County Oct. 18, 2000); *State of Oregon v. Ann Marie Eaton*, Case No. 002378FE (Jackson County Aug. 25, 2000); *State of Oregon v. Michael Scott Gilhousen*, Case No. 002225FE (Jackson County Nov. 7, 2000); *State of Oregon v. Robert Dean Golden*, Case No. 002726FE (Jackson County Oct. 18, 2000); *State of Oregon v. Annetta Lynn Kelley*, Case No. 002377FE (Jackson County July 24, 2000); *State of Oregon v. Gerald Jerome King*, Case No. 003594FE (Jackson County Oct. 31, 2000); *State of Oregon v. Micah John Right*, Case No. 002374FE (Jackson County Sept. 7, 2000); and *State of Oregon v. Todd Ivan Williams*, Case No. 004533FE (Jackson County Jan. 12, 2001).

4. Federal Credit Laws

It is important for training purposes and to assist victims in repairing damage to their credit history that prosecutors have at least a cursory understanding of credit laws that impact identity theft. The Fair Credit Reporting Act establishes procedures and time frames for correcting mistakes on credit records and requires that your record only be provided for legitimate business, credit, or employment needs. 15 U.S.C. § 1681 *et seq*. The Truth in Lending Act limits liability for unauthorized credit card charges in most cases to $50.00. 15 U.S.C. § 1601 *et seq*. The Fair Credit Billing Act establishes procedures for resolving billing errors on credit card accounts *if* the unauthorized charge is reported within certain time frames. 15 U.S.C. § 1666. The Fair Debt Collection Practices Act prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that your creditor has forwarded for collection. 15 U.S.C. § 1692. The Electronic Fund Transfer Act provides consumer protections for transactions using a debit card or electronic means to debit or credit an account. It also limits a consumer's liability for unauthorized electronic fund transfers *if* the unauthorized transfer is reported within certain time frames. 15 U.S.C. § 1693. If an ATM or debit card is reported lost or stolen within two business days of the loss or theft, the losses are limited to $50.00. If reported after two business days but within 60 days of the first statement showing an unauthorized transfer, the losses are limited to $500.00. Otherwise, losses may only be limited by the amount obtained. 15 U.S.C. § 1693(g)(a).

5. State Criminal Laws

Most states have laws prohibiting the theft of identity information. Where specific identity theft laws do not exist, the practices may be prohibited under other state laws or the states may be considering such legislation. The following is a list of current state laws which prohibit the theft of identity information: Ariz. Rev. Stat. § 13-2008; Ark. Code Ann. § 5-37-227; Cal. Penal Code § 530.5; 2000 Colo. Legis. Serv. ch 159 (May 19, 2000); 1999 Conn. Acts 99-99; Del. Code Ann. tit. 11, § 854; Fla. Stat. Ann. § 817.568; Ga. Code Ann. § 16-9-121 to 16-9-

127; Idaho Code § 18-3126; 720 Ill Comp.Stat. 5/16G; Ind.Code § 35-43-5-4 (2000); Iowa Code § 715A.8); Kan. Stat. Ann. § 21-4018; Ky. Rev. Stat. Ann. § 514.160; La. Rev. Stat. Ann. § 67.16; Me. Rev. Stat. Ann. tit. 17-A, § 354-2A; Md. Ann. Code art. 27, § 231; Mass. Gen. Laws ch. 266, § 37E; Minn. Stat. Ann. § 609.527; Miss. Code Ann. § 97-19-85; Mo. Rev. Stat. § 570.223; Neb. Rev. State. § 28-101; Nev. Rev. Stat. § 205.465; N.H. Rev. Stat. Ann. § 638:26; N.J. Stat. Ann. § 2C:21-17; N.C. Gen. Stat. § 14-113.20; N.D. Cent. Code § 12.1-23-11; Ohio Rev. Code Ann. 2913.49; Okla. Stat. tit. 21, § 1533.1; Or. Rev. Stat. § 165.800; Pa. Cons. Stat. Ann. § 420; R.I. Gen. Laws § 11-49.1-1; S.C. Code Ann. § 16-13-500; S.D. Codified Laws 20; Tenn. Code Ann. § 39-14-150; Tex. Penal Code Ann.§ 35.51; Utah Code Ann. § 76-6-1101-1104; VA. Code Ann. § 18.2-186.3; Wash. Rev. Code § 9.35; W. Va. Code Ann. § 61-3-54; Wis. Stat. § 943.201; Wyo. Stat. Ann. § 6-3-901.

How Can Identity Theft Be Prevented?

While it is extremely difficult to prevent identity theft, the best approach is to be proactive and take steps to avoid becoming a victim. As prosecutors, it is important to learn how to prevent identity theft in order to provide training to law enforcement and private industry. We can also complement the assistance to victims provided by our victim/witness units. A thorough guide to preventing and responding to identity theft can be found in Mari Frank and Beth Givens, *Privacy Piracy! A Guide to Protecting Yourself from Identity Theft*, Office Depot, (1999). Related information can be found at www.identitytheft.org. The FTC has also published a helpful guide entitled FTC, *ID Theft: When Bad Things Happen to Your Good Name*, (August 2000). This and related information can be found at www.consumer.gov/idtheft. Also, the United States Postal Inspection Service has produced an excellent video about identity theft entitled *IDENTITY THEFT: The Game of the Name*.

1. Only Share Identity Information When Necessary.

Be cautious about sharing personal information with anyone who does not have a legitimate need for the information. For instance, credit card numbers should never be provided to anyone over the telephone unless the consumer has initiated the call and is familiar with the entity with whom they are doing business. Likewise, SSNs should not be provided to anyone other than employers or financial institutions who need the SSN for wage, interest and tax reporting purposes. Businesses may legitimately inquire about a SSN if doing a credit check for purposes of financing a purchase. Some entities, however, may simply want the SSN for record-keeping purposes. Businesses may choose to not provide a service or benefit without obtaining a person's SSN, but the choice as to whom a SSN is provided should be exercised with caution. In the event an entity, such as a hospital or a Department of Motor Vehicles (DMV), assigns a SSN as a patient or client identification number, the customer should request that an alternative number be assigned.

2. When in Public, Exercise Caution When Providing Identity Information.

"Shoulder surfers" regularly glean such information for their fraudulent use. Be especially cautious when entering account information at an Automatic Teller Machine (ATM), or when entering long-distance calling card information on a public telephone. Likewise, be cautious when orally providing this type of information on a public telephone. Also, do not put identity information, such as an address or license plate number, on a key ring or anything similar that can easily be observed or lost. Identity information on such objects simply provides thieves easier means of finding and accessing homes and cars.

3. Do Not Carry Unnecessary Identity Information in a Purse or Wallet.

According to the FTC Identity Theft Clearinghouse, the primary means for thieves to obtain identity information is through the loss or theft of purses and wallets. To reduce the risk that identification information might be misappropriated, only carry the identity information necessary for use during the course of daily activities such as a driver's license, one credit or debit card, an insurance card, and membership cards that are regularly required for use. There should be no need to carry a Social

Security card, or anything containing a SSN. Likewise, there should be no need to carry a birth certificate or a passport. These items should be kept under lock and key in a safe or a safety deposit box. Credit or debit cards that are not regularly used should also be removed from a purse or wallet. The fewer pieces of identification carried in a purse or wallet, the easier it is to identify an individual piece that may have been lost or stolen, and the easier the task of notifying creditors and replacing such information should a purse or wallet be lost or stolen.

4. Secure Your Mailbox.

According to the FTC, the second most successful means for thieves to obtain identity information is through stolen mail. Many thieves follow letter carriers at a discreet distance and steal mail immediately after it has been delivered to a residential mail box. Do not place outgoing mail in residential mail boxes. Doing so, especially raising a red flag on a mail box to notify the postal carrier of outgoing mail, is simply an invitation to steal. Deposit outgoing mail in locked post office collection boxes or at a local post office. If you prefer to have mail delivered to your residential address, install a mail box which is secured by lock and key. Promptly remove mail after it has been delivered to your mailbox.

5. Secure Information on Your Personal Computer.

Similar to telephonic inquiries, credit card numbers should not be provided to anyone on the Internet unless the consumer has initiated the contact and is familiar with the entity with whom they are doing business. In addition to cautiously choosing with whom identity information is shared, computer users should install a firewall on their personal computers to prevent unauthorized access to stored information. A personal firewall is designed to run on an individual personal computer and isolate it from the rest of the Internet, thereby preventing unauthorized access to the computer. The user sets the level of desired security and the firewall inspects each packet of data to determine if it should be allowed to get to or from the individual machine, consistent with the level of security. A firewall is especially necessary for Digital Subscriber Line (DSL), cable modem, or other "always-on" connections. There are a number of quality firewall software applications that can be downloaded as freeware from sites on the Internet.

6. Keep Financial and Medical Records in a Secure Location.

Thieves may be more interested in identity information from which they can access credit, than in physical property. It is important, therefore, to keep all financial and medical records, and any other information containing identity information, in a secure location under lock and key.

7. Shred Nonessential Material Containing Identity Information.

All nonessential documentary material containing any type of identity information should be shredded prior to being placed in garbage or recycling. The term "nonessential" should be interpreted as anything that an individual or business is not required by law or policy to retain. For individuals this includes credit or debit card receipts, canceled bank checks and statements, outdated insurance or financial information, and junk mail, especially pre-approved credit applications and subscription solicitations. For businesses or medical facilities, this includes receipts of completed credit or debit card transactions, outdated client files, or prescription labels. The best shredding is done through a cross-cut shredder which cuts paper into small pieces, making it extremely difficult to reconstruct documents. Expired credit or debit cards should also be cut into several pieces before being discarded.

8. "Sanitize" the Contents of Garbage and Recycling.

All nonessential documentary material containing any type of identity information should be shredded before being placed in garbage or recycling. While junk mail or old financial documents may appear to be innocuous, they can be a gold mine when obtained by an identity thief.

9. Ensure That Organizations Shred Identity Information.

Many businesses, firms, and medical facilities are not sensitive to privacy issues arising from discarded material. Many of these entities regularly dispose of material containing customer identity information, i.e. customer orders, receipts, prescription labels, etc., into garbage cans, dumpsters, or recycling bins without shredding the material. Tremendous damage can be done by these practices. Customers of businesses, clients of firms, and patients of medical facilities should insist that all data be shredded before being discarded and that all retained data be kept in secure storage.

10. Remove Your Name from Mailing Lists.

Removing a name from a mailing list reduces the number of commercial entities having access to the identity information. It also reduces the amount of junk mail, including pre-approved credit applications and subscription solicitations, thereby reducing the risk that the theft of such mail will compromise privacy. Many financial institutions, such as banks and credit card companies, and even state agencies, market identity information of customers unless a request is received, in writing, that such information is not to be shared. Customers of such businesses and agencies should submit such requests, notifying the entity in writing of their desire to opt out of any mailing lists, and to not have identity information shared.

To opt out of the mailing lists of the three major credit bureaus (Equifax, Experian, and Trans Union), call 1-888-5OPT-OUT. To opt out of many national direct mail lists, write the Direct Marketing Association, DMA Preference Service, P.O. Box 9008, Farmingdale, N.Y. 11735-9008. To opt out of many national direct e-mail lists, visit www.e-mps.org. To opt out of many national telemarketer lists, send your name, address and telephone number to the Direct Marketing Association, DMA Telephone Preference Service, P.O. Box 9014, Farmingdale, N.Y. 11735-9014.

11. Carefully Review Financial Statements.

Promptly review all bank and credit card statements for accuracy. Pay attention to billing cycles. A missing bill may mean a thief has taken over an account and changed the billing address to avoid detection. Report any irregularities to the bank or credit card company immediately.

12. Periodically Request Copies of Credit Reports.

Credit reports are available for $8.00 from the three major credit bureaus (Equifax, Experian, and Trans Union). Credit bureaus must provide a free copy of the report if it is inaccurate due to fraud and it is requested in writing. The reports should be reviewed carefully to make sure no unauthorized accounts have been opened or unauthorized changes made to existing accounts.

To order a report from Equifax, visit www.equifax.com, call 1-800-685-1111 or write P.O. Box 740241, Atlanta, GA 30374-0241. To order a report from Experian, visit www.experian.com, call 1-888-EXPERIAN (397-3742) or write P.O. Box 949, Allen, TX 75013- 0949. To order a report from Trans Union, visit www.tuc.com, call 800-916-8800 or write P.O. Box 1000, Chester, PA 19022.

What Steps Should Be Taken by a Victim of Identity Theft?

When someone realizes they have become a victim of identity theft, they should take the following steps while keeping a log of all conversations, including dates, names, and telephone numbers. The log should indicate any time spent and expenses incurred in the event restitution can be obtained in a civil or criminal judgment against the thief. All conversations should be confirmed in writing with the correspondence sent by certified mail, return receipt requested. All correspondence should be kept in a secure location, under lock and key.

First, the victim should contact the fraud departments of each of the three major credit bureaus (Equifax, Experian, and Trans Union), inform the representative of the identity theft, and request that a “fraud alert” be placed on their file, as well as a statement asking that creditors call the victim before opening any new accounts. This can help prevent an identity thief from opening additional accounts in the victim’s name. The victim should inquire about how long the fraud alert will remain on the file, and what, if anything, must be done to extend the alert if necessary. Copies of credit reports from the credit bureaus

should also be ordered. The reports should be reviewed carefully to identify unauthorized accounts or unauthorized changes to existing accounts. Also, if the reports indicate that any "inquiries" were made from companies that opened fraudulent accounts, a request should be made to remove the "inquiries" from the report. A request should also be made for the credit bureaus to notify those who have received a credit report in the last six months and alert them to the disputed and erroneous information. The victim should request a new copy of the reports after a few months, to verify that the requested changes have been made, and to ensure no new fraudulent activity has occurred.

To report fraud to Equifax, visit www.equifax.com, call 1-800-525-6285 and write P.O. Box 740241, Atlanta, GA 30374-0241. To report fraud to Experian, visit www.experian.com, call 1-888-EXPERIAN and write P.O. Box 949, Allen TX 75013-0949. To report fraud to Trans Union, visit www.tuc.com, call 1-800-680-7289 and write Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634.

Second, the victim should contact the security or fraud departments for any creditors of accounts in which fraudulent activity occurred. The telephone numbers for these creditors can be obtained from the credit bureaus. Creditors can include businesses, credit card companies, telephone companies and other utilities, and banks and other lenders. All conversations should be confirmed with written correspondence. It is particularly important to notify credit card companies in writing because it is required by the consumer protection laws set forth above. The victim should immediately close accounts that have been tampered with and open new ones with new Personal Identification Numbers (PINs) and passwords.

Third, the victim should file a report with a local police department or the police department where the identity theft occurred, if that can be determined. The victim should obtain a copy of the police report in the event creditors need proof of the crime. Even if the thief is not apprehended, a copy of the police report may assist the victim when dealing with creditors. The victim should also file a complaint with the FTC. The FTC should be contacted on its Identity Theft Hotline toll free at 1-877-ID THEFT (438-4338), TDD at 1-202-326-2502, by mail at FTC Identity Theft Clearinghouse, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580, or at www.consumer.gov/idtheft.

Fourth, certain situations may require additional action by the victim. For instance, if an identity thief has stolen mail, it should be reported to a local postal inspector. A phone number for the nearest postal inspection service office can be obtained from a local post office or the U.S. Postal Service web site at www.usps.com/postalinspectors. If financial information has been obtained, the financial entity (the bank, brokerage firm, credit union, credit card company, etc.) should be contacted, the fraudulently affected accounts closed, and new accounts opened with new PINs and passwords, including affected ATM cards. Payment should be stopped on any stolen checks, and banks or credit unions should be asked to request the appropriate check verification service to notify retailers not to accept the checks. Three check verification companies that accept reports of check fraud directly from consumers are: Telecheck: 1-800-710-9898; International Check Services: 1-800-631-9656; and Equifax: 1-800-437-5120. If investments or securities may have been affected, brokers should be notified and the victim should file a complaint with the Securities and Exchange Commission (SEC). A complaint can be filed with the SEC at the SEC Enforcement Complaint Center, 450 Fifth Street, NW, Washington, D.C. 20549-0202; its web site www.sec.gov, e-mail enforcement@sec.gov, or fax (202) 942-9570.

If new phone service has fraudulently been established in a victim's name or billing for unauthorized service is made to an existing account, the victim should contact the service provider immediately to cancel the account and/or calling card and open new accounts with new PINs and passwords. If a victim has difficulty removing fraudulent charges from an account, a complaint should be filed with the Federal Communications Commission (FCC). A complaint can be filed with the FCC at the FCC Consumer Information Bureau, 445 12th Street,

S.W., Room 5A863, Washington, DC 20554; the FCC Enforcement Bureau web site www.fcc.gov/eb, e-mail fccinfo@fcc.gov, telephone 1-888-CALL FCC, or TTY 1-888-TELL FCC.

If someone is using a victim's SSN to apply for a job or to work, it should be reported to the Social Security Administration (SSA). The victim should first visit the SSA's web site at www.ssa.gov, read the Guidelines for Reporting Fraud, Waste, Abuse and Mismanagement, and then call the SSA Fraud Hotline at 1-800-269-0271, and file a report at SSA Fraud Hotline, P.O. Box 17768, Baltimore MD 21235, fax 410-597-0118 or e-mail oig.hotline@ssa.gov. The victim should also call the SSA at 1-800-772-1213 to verify the accuracy of earnings reported under the SSN and to request a copy of the victim's Social Security Personal Earnings and Benefit Estimate Statement. The Statement should reveal earnings posted to the victim's SSN by the identity thief. If an SSN has been fraudulently used, the Internal Revenue Service (IRS) Taxpayer Advocates Office should be contacted. The fraudulent use of an SSN might result in what appears to be an underreporting of a victim's taxable income and an attempt by the IRS to collect taxes on the underreported income. The IRS Taxpayer Advocates Office can be contacted at 1-877-777-4778 or www.treas.gov/irs/ci.

If someone has fraudulently obtained a driver's license or photographic identification card in a victim's name through an office of a DMV, the local DMV should be contacted and a fraud alert should be placed in the license. Likewise, if someone has stolen any other identification document, the entity responsible for creating the document should be contacted and informed of the theft. If a passport has been lost or stolen, the United States State Department should be contacted at Passport Services, Correspondence Branch, 1111 19th Street, NW, Suite 510 Washington, DC 20036, or www.travel.state.gov/passport_services. If someone has stolen a health insurance card, the theft should be reported to the insurer. Subsequent insurance statements should be reviewed for fraudulent billing.

If someone has fraudulently filed for bankruptcy in a victim's name, the U.S. Trustee should be contacted in the region where the bankruptcy was filed. A listing of the U.S. Trustees can be found at www.usdoj.gov/ust. A written complaint must be filed describing the situation and providing proof of the victim's identity. The U.S. Trustee, if appropriate, will make a referral to criminal law enforcement authorities. The victim should also file a complaint with the FBI in the city where the bankruptcy was filed.

In rare instances, an identity thief may create a criminal record under a victim's name by providing the identity when arrested. Victims of this type of problem should contact the FBI and initiate a request that the victim's name be cleared, and retain an attorney to resolve the problem as procedures for clearing one's name may vary by jurisdiction.

Conclusion

Identity theft was clearly identified as a serious crime two years ago when the Identity Theft Act was passed. Since that time great strides have been made to combat the problem, but much work remains to be done. Law enforcement agencies at all levels, federal and non-federal, must work together to develop strategies for the investigation and prosecution of offenders. At the same time, the law enforcement community must work closely with private industry to develop effective education and prevention programs. The crime of the new millennium will not fade away soon, nor will passive efforts soften the devastating impact upon its victims. Yet with hard work, cooperation, and effective communication between law enforcement and the public, identity thieves will be held accountable in this new millennium. ~

ABOUT THE AUTHOR

‘ **Sean B. Hoar** has been an AUSA since 1991 and is the Computer and Telecommunications Coordinator (CTC) for the southern half of the District of Oregon. As such, he prosecuted the first case in the United States under the No Electronic Theft Act (NET Act) involving criminal copyright infringement on the Internet. He is primarily concerned with developing partnerships with local, state and federal law enforcement agencies to prevent, investigate and prosecute cyber crime. Previously he was primarily involved in the prosecution of organizational narcotics traffickers and received the Directors Award for his role in prosecuting a heroin trafficking organization based in Southeast Asia which included a General in the Royal Thai Army who was a member of the Supreme Command of the Royal Thai Armed Forces. **a**

Computer Records and the Federal Rules of Evidence

Orin S. Kerr
Trial Attorney
Computer Crime and Intellectual Property Section

This article explains some of the important issues that can arise when the government seeks the admission of computer records under the Federal Rules of Evidence. It is an excerpt of a larger DOJ manual entitled "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", which is available on the internet at www.cybercrime.gov/searchmanual.htm.

Most federal courts that have evaluated the admissibility of computer records have focused on computer records as potential hearsay. The courts generally have admitted computer records upon a showing that the records fall within the business records exception, Fed. R. Evid. 803(6):

> **Records of regularly conducted activity**. A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term “business” as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

See, e.g., *United States v. Cestnik*, 36 F.3d 904, 909-10 (10th Cir. 1994); *United States v. Moore*, 923 F.2d 910, 914 (1st Cir. 1991); *United States v. Briscoe*, 896 F.2d 1476, 1494 (7th Cir. 1990); *United States v. Catabran*, 836 F.2d 453, 457 (9th Cir. 1988); *Capital Marine Supply v. M/V Roland Thomas II*, 719 F.2d 104, 106 (5th Cir. 1983). Applying this test, the courts have indicated that computer records generally can be admitted as business records if they were kept pursuant to a routine procedure for motives that tend to assure their accuracy.

However, the federal courts are likely to move away from this “one size fits all” approach as they become more comfortable and familiar with computer records. Like paper records, computer records are not monolithic: the evidentiary issues raised by their admission should depend on what

kind of computer records a proponent seeks to have admitted. For example, computer records that contain text often can be divided into two categories: computer-generated records, and records that are merely computer-stored. *See People v. Holowko*, 486 N.E.2d 877, 878-79 (Ill. 1985). The difference hinges upon whether a person or a machine created the records' contents. Computer-stored records refer to documents that contain the writings of some person or persons and happen to be in electronic form. E-mail messages, word processing files, and Internet chat room messages provide common examples. As with any other testimony or documentary evidence containing human statements, computer-stored records must comply with the hearsay rule. If the records are admitted to prove the truth of the matter they assert, the offeror of the records must show circumstances indicating that the human statements contained in the record are reliable and trustworthy, *see* Advisory Committee Notes to Proposed Rule 801 (1972), and the records must be authentic.

In contrast, computer-generated records contain the output of computer programs, untouched by human hands. Log-in records from Internet service providers, telephone records, and ATM receipts tend to be computer-generated records. Unlike computer-stored records, computer-generated records do not contain human "statements," but only the output of a computer program designed to process input following a defined algorithm. Of course, a computer program can direct a computer to generate a record that mimics a human statement: an e-mail program can announce "You've got mail!" when mail arrives in an inbox, and an ATM receipt can state that $100 was deposited in an account at 2:25 pm. However, the fact that a computer, rather than a human being, has created the record alters the evidentiary issues that the computer-generated records present. *See, e.g.*, 2 J. Strong, *McCormick on Evidence* § 294, at 286 (4th ed. 1992). The evidentiary issue is no longer whether a human's out-of-court statement was truthful and accurate (a question of hearsay), but instead whether the computer program that generated the record was functioning properly (a question of authenticity). *See id*.; Richard O. Lempert & Steven A. Saltzburg, *A Modern Approach to Evidence* 370 (2d ed. 1983); *Holowko*, 486 N.E.2d at 878-79.

Finally, a third category of computer records exists: some computer records are both computer-generated *and* computer-stored. For example, a suspect in a fraud case might use a spreadsheet program to process financial figures relating to the fraudulent scheme. A computer record containing the output of the program would derive from both human statements (the suspect's input to the spreadsheet program) and computer processing (the mathematical operations of the spreadsheet program). Accordingly, the record combines the evidentiary concerns raised by computer-stored and computer-generated records. The party seeking the admission of the record should address both the hearsay issues implicated by the original input and the authenticity issues raised by the computer processing.

As the federal courts develop a more nuanced appreciation of the distinctions to be made between different kinds of computer records, they are likely to see that the admission of computer records generally raises two distinct issues. First, the government must establish the authenticity of all computer records by providing "evidence sufficient to support a finding that the matter in question is what its proponent claims." Fed. R. Evid. 901(a). Second, if the computer records are computer-stored records that contain human statements, the government must show that those human statements are not inadmissible hearsay.

A. Authentication

Before a party may move for admission of a computer record or any other evidence, the proponent must show that it is authentic. That is, the government must offer evidence "sufficient to support a finding that the [computer record or other evidence] in question is what its proponent claims." Fed. R. Evid. 901(a). *See United States v. Simpson*, 152 F.3d 1241, 1250 (10th Cir. 1998).

The standard for authenticating computer records is the same as for authenticating other records. The degree of authentication does not vary simply because a record happens to be (or has been at one point) in electronic form. *See United States v. DeGeorgia*, 420 F.2d 889, 893

n.11 (9th Cir. 1969); *United States v. Vela*, 673 F.2d 86, 90 (5th Cir. 1982). *But see United States v. Scholle*, 553 F.2d 1109, 1125 (8th Cir. 1977) (stating in *dicta* that "the complex nature of computer storage calls for a more comprehensive foundation"). For example, witnesses who testify to the authenticity of computer records need not have special qualifications. The witness does not need to have programmed the computer himself, or even need to understand the maintenance and technical operation of the computer. *See United States v. Moore*, 923 F.2d 910, 915 (1st Cir. 1991) (citing cases). Instead, the witness simply must have first-hand knowledge of the relevant facts to which he or she testifies. *See generally United States v. Whitaker*, 127 F.3d 595, 601 (7th Cir. 1997) (FBI agent who was present when the defendant's computer was seized can authenticate seized files) *United States v. Miller*, 771 F.2d 1219, 1237 (9th Cir. 1985) (telephone company billing supervisor can authenticate phone company records); *Moore*, 923 F.2d at 915 (head of bank's consumer loan department can authenticate computerized loan data).

Challenges to the authenticity of computer records often take one of three forms. First, parties may challenge the authenticity of both computer-generated and computer-stored records by questioning whether the records were altered, manipulated, or damaged after they were created. Second, parties may question the authenticity of computer-generated records by challenging the reliability of the computer program that generated the records. Third, parties may challenge the authenticity of computer-stored records by questioning the identity of their author.

1. Authenticity and the Alteration of Computer Records

Computer records can be altered easily, and opposing parties often allege that computer records lack authenticity because they have been tampered with or changed after they were created. For example, in *United States v. Whitaker*, 127 F.3d 595, 602 (7th Cir. 1997), the government retrieved computer files from the computer of a narcotics dealer named Frost. The files from Frost's computer included detailed records of narcotics sales by three aliases: "Me" (Frost himself, presumably), "Gator" (the nickname of Frost's co-defendant Whitaker), and "Cruz" (the nickname of another dealer). After the government permitted Frost to help retrieve the evidence from his computer and declined to establish a formal chain of custody for the computer at trial, Whitaker argued that the files implicating him through his alias were not properly authenticated. Whitaker argued that "with a few rapid keystrokes, Frost could have easily added Whitaker's alias, 'Gator' to the printouts in order to finger Whitaker and to appear more helpful to the government." *Id*. at 602.

The courts have responded with considerable skepticism to such unsupported claims that computer records have been altered. Absent specific evidence that tampering occurred, the mere possibility of tampering does not affect the authenticity of a computer record. *See Whitaker*, 127 F.3d at 602 (declining to disturb trial judge's ruling that computer records were admissible because allegation of tampering was "almost wild-eyed speculation . . . [without] evidence to support such a scenario"); *United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1988) ("The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness."); *United States v. Glasser*, 773 F.2d 1553, 1559 (11th Cir. 1985) ("The existence of an air-tight security system [to prevent tampering] is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records; the party opposing admission would have to show only that a better security system was feasible."). *Id.* at 559. This is consistent with the rule used to establish the authenticity of other evidence such as narcotics. *See United States v. Allen*, 106 F.3d 695, 700 (6th Cir. 1997) ("Merely raising the possibility of tampering is insufficient to render evidence inadmissible."). Absent specific evidence of tampering, allegations that computer records have been altered go to their weight, not their admissibility. *See Bonallo*, 858 F.2d at 1436.

2. Establishing the Reliability of Computer Programs

The authenticity of computer-generated records sometimes implicates the reliability of the computer programs that create the records. For example, a computer-generated record might not be authentic if the program that creates the record contains serious programming errors. If the program's output is inaccurate, the record may not be "what its proponent claims" according to Fed. R. Evid. 901.

Defendants in criminal trials often attempt to challenge the authenticity of computer-generated records by challenging the reliability of the programs. *See, e.g.*, *United States v. Dioguardi*, 428 F.2d 1033, 1038 (2d Cir. 1970); *United States v. Liebert*, 519 F.2d 542, 547-48 (3d Cir. 1975). The courts have indicated that the government can overcome this challenge so long as "the government provides sufficient facts to warrant a finding that the records are trustworthy and the opposing party is afforded an opportunity to inquire into the accuracy thereof[.]" *United States v. Briscoe*, 896 F.2d 1476, 1494 (7th Cir. 1990). *See also Liebert*, 519 F.2d at 547; *DeGeorgia*, 420 F.2d. at 893 n.11. *Compare* Fed. R. Evid. 901(b)(9) (indicating that matters created according to a process or system can be authenticated with "[e]vidence describing a process or system used . . . and showing that the process or system produces an accurate result"). In most cases, the reliability of a computer program can be established by showing that users of the program actually do rely on it on a regular basis, such as in the ordinary course of business. *See, e.g.*, *United States v. Moore*, 923 F.2d 910, 915 (1st Cir. 1991) ("[T]he ordinary business circumstances described suggest trustworthiness, . . . at least where absolutely nothing in the record in any way implies the lack thereof.") (computerized tax records held by the IRS); *Briscoe*, 896 F.2d at 1494 (computerized telephone records held by Illinois Bell). When the computer program is not used on a regular basis and the government cannot establish reliability based on reliance in the ordinary course of business, the government may need to disclose "what operations the computer had been instructed to perform [as well as] the precise instruction that had been given" if the opposing party requests. *Dioguardi*, 428 F.2d at 1038. Notably, once a minimum standard of trustworthiness has been established, questions as to the accuracy of computer records "resulting from . . . the operation of the computer program" affect only the weight of the evidence, not its admissibility. *United States v. Catabran*, 836 F.2d 453, 458 (9th Cir. 1988).

Prosecutors may note the conceptual overlap between establishing the authenticity of a computer-generated record and establishing the trustworthiness of a computer record for the business record exception to the hearsay rule. In fact, federal courts that evaluate the authenticity of computer-generated records often assume that the records contain hearsay, and then apply the business records exception. *See*, *e.g.*, *United States v. Linn*, 880 F.2d 209, 216 (9th Cir. 1989) (applying business records exception to telephone records generated "automatically" by a computer); *United States v. Vela*, 673 F.2d 86, 89-90 (5th Cir. 1982) (same). As discussed later in this article, this analysis is technically incorrect in many cases: computer records generated entirely by computers cannot contain hearsay and cannot qualify for the business records exception because they do not contain human "statements." *See* Part B, *infra*. As a practical matter, however, prosecutors who lay a foundation to establish a computer-generated record as a business record will also lay the foundation to establish the record's authenticity. Evidence that a computer program is sufficiently trustworthy so that its results qualify as business records according to Fed. R. Evid. 803(6) also establishes the authenticity of the record. *Compare United States v. Saputski*, 496 F.2d 140, 142 (9th Cir. 1974).

3. Identifying the Author of Computer-Stored Records

Although handwritten records may be penned in a distinctive handwriting style, computer-stored records consist of a long string of zeros and ones that do not necessarily identify their author. This is a particular problem with Internet communications, which offer their authors an unusual degree of anonymity. For example, Internet technologies permit users to send effectively anonymous e-mails, and Internet Relay Chat channels permit users to communicate

without disclosing their real names. When prosecutors seek the admission of such computer-stored records against a defendant, the defendant may challenge the authenticity of the record by challenging the identity of its author.

Circumstantial evidence generally provides the key to establishing the authorship and authenticity of a computer record. For example, in *United States v. Simpson*, 152 F.3d 1241 (10th Cir. 1998), prosecutors sought to show that the defendant had conversed with an undercover FBI agent in an Internet chat room devoted to child pornography. The government offered a printout of an Internet chat conversation between the agent and an individual identified as "Stavron," and sought to show that "Stavron" was the defendant. The district court admitted the printout in evidence at trial. On appeal following his conviction, Simpson argued that "because the government could not identify that the statements attributed to [him] were in his handwriting, his writing style, or his voice," the printout had not been authenticated and should have been excluded. *Id*. at 1249.

The Tenth Circuit rejected this argument, noting the considerable circumstantial evidence that "Stavron" was the defendant. *See id*. at 1250. For example, "Stavron" had told the undercover agent that his real name was "B. Simpson," gave a home address that matched Simpson's, and appeared to be accessing the Internet from an account registered to Simpson. Further, the police found records in Simpson's home that listed the name, address, and phone number that the undercover agent had sent to "Stavron." Accordingly, the government had provided evidence sufficient to support a finding that the defendant was "Stavron," and the printout was properly authenticated. *See id.* at 1250. *See also United States v. Tank*, 200 F.3d 627, 630-31 (9th Cir. 2000) (concluding that district court properly admitted chat room log printouts in circumstances similar to those in *Simpson*). *But see United States v. Jackson*, 208 F.3d 638 (7th Cir. 2000) (concluding that web postings purporting to be statements made by white supremacist groups were properly excluded on authentication grounds absent evidence that the postings were actually posted by the groups).

B. Hearsay

Federal courts have often assumed that all computer records contain hearsay. A more nuanced view suggests that in fact only a portion of computer records contain hearsay. When a computer record contains the assertions of a person, whether or not processed by a computer, the record can contain hearsay. In such cases, the government must fit the record within a hearsay exception such as the business records exception, Fed. R. Evid. 803(6). When a computer record contains only computer-generated data untouched by human hands, however, the record cannot contain hearsay. In such cases, the government must establish the authenticity of the record, but does not need to establish that a hearsay exception applies for the records to be admissible.

1. Inapplicability of the Hearsay Rules to Computer-Generated Records

The hearsay rules exist to prevent unreliable out-of-court statements by human declarants from improperly influencing the outcomes of trials. Because people can misinterpret or misrepresent their experiences, the hearsay rules express a strong preference for testing human assertions in court, where the declarant can be placed on the stand and subjected to cross-examination. *See Ohio v. Roberts*, 448 U.S. 56, 62-66 (1980). This rationale does not apply when an animal or a machine makes an assertion: beeping machines and barking dogs cannot be called to the witness stand for cross-examination at trial. The Federal Rules have adopted this logic. By definition, an assertion cannot contain hearsay if it was not made by a human being. Can we just use the word person? *See* Fed. R. Evid. 801(a) ("A 'statement' is (1) an oral or written assertion or (2) nonverbal conduct *of a person*, if it is intended by the person as an assertion.") (emphasis added) ; Fed. R. Evid. 801(b) ("A declarant is *a person* who makes a statement.") (emphasis added).

As several courts and commentators have noted, this limitation on the hearsay rules necessarily means that computer-generated records untouched by human hands cannot contain hearsay. One state supreme court articulated the distinction in an early case involving the use of automated telephone records:

> The printout of the results of the computer's internal operations is not hearsay evidence. It does not represent the output of statements placed into the computer by out of court declarants. Nor can we say that this printout itself is a "statement" constituting hearsay evidence. The underlying rationale of the hearsay rule is that such statements are made without an oath and their truth cannot be tested by cross-examination. Of concern is the possibility that a witness may consciously or unconsciously misrepresent what the declarant told him or that the declarant may consciously or unconsciously misrepresent a fact or occurrence. With a machine, however, there is no possibility of a conscious misrepresentation, and the possibility of inaccurate or misleading data only materializes if the machine is not functioning properly.

State v. Armstead, 432 So.2d 837, 840 (La. 1983). *See also People v. Holowko*, 486 N.E.2d 877, 878-79 (Ill. 1985) (automated trap and trace records); *United States v. Duncan*, 30 M.J. 1284, 1287-89 (N-M.C.M.R. 1990) (computerized records of ATM transactions); 2 J. Strong, *McCormick on Evidence* § 294, at 286 (4th ed.1992); Richard O. Lempert & Stephen A. Saltzburg, *A Modern Approach to Evidence* 370 (2d ed. 1983). *Cf. United States v. Fernandez-Roque*, 703 F.2d 808, 812 n.2 (5th Cir. 1983) (rejecting hearsay objection to admission of automated telephone records because "the fact that these calls occurred is not a hearsay statement."). Accordingly, a properly authenticated computer-generated record is admissible. *See* Lempert & Saltzburg, at 370.

The insight that computer-generated records cannot contain hearsay is important because courts that assume the existence of hearsay may wrongfully exclude computer-generated evidence if a hearsay exception does not apply. For example, in *United States v. Blackburn*, 992 F.2d 666 (7th Cir. 1993), a bank robber left his eyeglasses behind in an abandoned stolen car. The prosecution's evidence against the defendant included a computer printout from a machine that tests the curvature of eyeglass lenses. The printout revealed that the prescription of the eyeglasses found in the stolen car exactly matched the defendant's. At trial, the district court assumed that the computer printout was hearsay, but concluded that the printout was an admissible business record according to Fed. R. Evid. 803(6). On appeal following conviction, the Seventh Circuit also assumed that the printout contained hearsay, but agreed with the defendant that the printout could not be admitted as a business record:

> the [computer-generated] report in this case was not kept in the course of a regularly conducted business activity, but rather was specially prepared at the behest of the FBI and with the knowledge that any information it supplied would be used in an ongoing criminal investigation. . . . In finding this report inadmissible under Rule 803(6), we adhere to the well-established rule that documents made in anticipation of litigation are inadmissible under the business records exception.

Id. at 670. *See also* Fed. R. Evid. 803(6) (stating that business records must be "made . . . by, or transmitted by, a person").

Fortunately, the *Blackburn* court ultimately affirmed the conviction, concluding that the computer printout was sufficiently reliable that it could have been admitted under the residual hearsay exception, Rule 803(24). *See id*. at 672. However, instead of flirting with the idea of excluding the printouts because Rule 803(6) did not apply, the court should have asked whether the computer printout from the lens-testing machine contained hearsay at all. This question would have revealed that the computer-generated printout could not be excluded on hearsay grounds because it contained no human "statements."

2. Applicability of the Hearsay Rules to Computer-Stored Records

Computer-stored records that contain human statements must satisfy an exception to the hearsay rule if they are offered for the truth of the matter asserted. Before a court will admit the records, the court must establish that the statements contained in the record were made in circumstances that tend to ensure their

trustworthiness. *See, e.g., Jackson*, 208 F.3d at 637 (concluding that postings from the websites of white supremacist groups contained hearsay, and rejecting the argument that the postings were the business records of the ISPs that hosted the sites).

As discussed earlier in this article, courts generally permit computer-stored records to be admitted as business records according to Fed. R. Evid. 803(6). Different circuits have articulated slightly different standards for the admissibility of computer-stored business records. Some courts simply apply the direct language of Fed. R. Evid. 803(6). *See e.g.,United States v. Moore*, 923 F.2d 910, 914 (1st Cir. 1991); *United States v. Catabran*, 836 F.2d 453, 457 (9th Cir. 1988). Other circuits have articulated doctrinal tests specifically for computer records that largely (but not exactly) track the requirements of Rule 803(6). *See, e.g., United States v. Cestnik*, 36 F.3d 904, 909-10 (10th Cir. 1994) ("Computer business records are admissible if (1) they are kept pursuant to a routine procedure designed to assure their accuracy; (2) they are created for motives that tend to assure accuracy (e.g., not including those prepared for litigation); and (3) they are not themselves mere accumulations of hearsay.") (quoting *Capital Marine Supply v. M/V Roland Thomas II*, 719 F.2d 104, 106 (5th Cir. 1983)); *United States v. Briscoe*, 896 F.2d 1476, 1494 (7th Cir. 1990) (computer-stored records are admissible business records if they "are kept in the course of regularly conducted business activity, and [that it] was the regular practice of that business activity to make records, as shown by the testimony of the custodian or other qualified witness.") (*quoting United States v. Chappell*, 698 F.2d 308, 311 (7th Cir. 1983)). Notably, the printout itself may be produced in anticipation of litigation without running afoul of the business records exception. The requirement that the record be kept "in the course of a regularly conducted business activity" refers to the underlying data, not the actual printout of that data. *See United States v. Sanders*, 749 F.2d 195, 198 (5th Cir. 1984).

From a practical perspective, the procedure for admitting a computer-stored record pursuant to the business records exception is the same as admitting any other business record. Consider an e-mail harassment case. To help establish that the defendant was the sender of the harassing messages, the prosecution may seek the introduction of records from the sender's ISP showing that the defendant was the registered owner of the account from which the e-mails were sent. Ordinarily, this will require testimony from an employee of the ISP ("the custodian or other qualified witness") that the ISP regularly maintains customer account records for billing and other purposes, and that the records to be offered for admission are such records that were made at or near the time of the events they describe in the regular course of the ISP's business. Again, the key is establishing that the computer system from which the record was obtained is maintained in the ordinary course of business, and that it is a regular practice of the business to rely upon those records for their accuracy.

The business record exception is the most common hearsay exception applied to computer records. Of course, other hearsay exceptions may be applicable in appropriate cases. *See, e.g., Hughes v. United States*, 953 F.2d 531, 540 (9th Cir. 1992) (concluding that computerized IRS forms are admissible as public records under Fed. R. Evid. 803(8)).

C. Other Issues

The authentication requirement and the hearsay rule usually provide the most significant hurdles that prosecutors will encounter when seeking the admission of computer records. However, some agents and prosecutors have occasionally considered two additional issues: the application of the best evidence rule to computer records, and whether computer printouts are "summaries" that must comply with Fed. R. Evid. 1006.

1. The Best Evidence Rule

The best evidence rule states that to prove the content of a writing, recording, or photograph, the "original" writing, recording, or photograph is ordinarily required. *See* Fed. R. Evid. 1002. Agents and prosecutors occasionally express concern that a mere printout of a computer-stored

electronic file may not be an "original" for the purpose of the best evidence rule. After all, the original file is merely a collection of 0's and 1's. In contrast, the printout is the result of manipulating the file through a complicated series of electronic and mechanical processes.

Fortunately, the Federal Rules of Evidence have expressly addressed this concern. The Federal Rules state that

> [i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original".

Fed. R. Evid. 1001(3). Thus, an accurate printout of computer data always satisfies the best evidence rule. *See Doe v. United States*, 805 F. Supp. 1513, 1517 (D. Hawaii. 1992). According to the Advisory Committee Notes that accompanied this rule when it was first proposed, this standard was adopted for reasons of practicality. While strictly speaking the original of a photograph might be thought to be only the negative, practicality and common usage require that any print from the negative be regarded as an original. Similarly, practicality and usage confer the status of original upon any computer printout. Advisory Committee Notes, Proposed Federal Rule of Evidence 1001(3) (1972).

2. Computer Printouts as "Summaries"

Federal Rule of Evidence 1006 permits parties to offer summaries of voluminous evidence in the form of "a chart, summary, or calculation" subject to certain restrictions. Agents and prosecutors occasionally ask whether a computer printout is necessarily a "summary" of evidence that must comply with Fed. R. Evid. 1006. In general, the answer is no. *See Sanders*, 749 F.2d at 199; *Catabran*, 836 F.2d at 456-57; *United States v. Russo*, 480 F.2d 1228, 1240-41 (6th Cir. 1973). Of course, if the computer printout is merely a summary of other admissible evidence, Rule 1006 will apply just as it does to other summaries of evidence.

ABOUT THE AUTHOR

Orin S. Kerr is a Trial Attorney, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice.

Gambling Against Enforcement — Internet Sports Books and the Wire Wager Act

Joseph V. DeMarco
Assistant United States Attorney
Southern District of New York

I. Introduction

Even as a certain "Madness" crowds network airwaves during the month of March, and as Americans gamble in various forms in ever-increasing numbers, gambling on sporting events is strictly regulated and, in most cases, prohibited outright under federal and state law. Notwithstanding these general prohibitions, however, the exponential growth in the use of the Internet by the mass public has been accompanied by a corresponding growth in the creation of Internet websites which offer Americans the ability to gamble on-line without the need for a neighborhood bookie. From on-line private lotteries, to on-line card games, "quiz shows," and traditional sports books, these websites offer privacy and anonymity to both the owners of the sites and their "clients" while, paradoxically, offering a perceived aura of legitimacy that derives from the fact that anyone can "sign on" to and use them as freely as any legitimate e-commerce site.

This article examines one form of gambling website — the Internet sports book — and the application of the Wire Wager Act, 18 U.S.C. § 1084, to enforcement operations directed against the operators of those websites. It will demonstrate that, notwithstanding the novel form that they take, these web-based books are fundamentally no different than bookmaking operations run by traditional "pay phone" bookies, and that there is no reason why the Wire Wager Act should not apply to such high-tech Internet bookies. The article will also examine why recurring arguments that seek to preclude application of the Wire Wager Act to Internet bookmakers — many of which can be, and often are, made in defense to prosecution of crimes committed via the Internet under other federal statutes — are unpersuasive.

II. The Rise Of The Internet Sports book

In the last several years, dozens of Internet sports books have sprung into existence. Many are located offshore, in Central American countries or on Carribean island nations where their bookmaking activities are not illegal. Notably, however, these sports books are frequently run by Americans and direct their activities to bettors in America interested in gambling on American sporting events such as baseball, football, and basketball. Typically, the books accept bets only in U.S. currency, and further require that all wagering be done from pre-funded betting "accounts." Toward this end, their websites provide instructions to bettors on how to wire transfer money to the sports books. Many advertise in U.S. magazines especially devoted to sports fans, in college newspapers, or on websites devoted to gambling generally or sports betting in particular. Indeed, some sports books' advertisements have represented that their operations are legal, and have sought to reassure bettors that they can be trusted because they hold licenses from, and are regulated by, their host countries. While some sports books operate entirely through Internet transmissions, others publish toll-free telephone numbers on their websites or in advertisements so that bettors can, if they choose, call and place wagers with a live operator. Notably, although many Internet sportsbooks purport to accept wagers only from persons having the legal capacity to gamble, the fact that most permit betting to be done anonymously or through pseudonyms precludes meaningful control of gambling by minors, much

less by persons who are intoxicated, or by persons with gambling addictions.

While precise data regarding the scale of illegal activities is obviously difficult to obtain, illegal Internet sports gambling by Americans was estimated by *Sports Illustrated* in 1998 to exceed $600 million, with a ten-fold increase predicted by 2001. Indeed, in a recent trial of a sports book operator brought in the Southern District of New York involving an Antigua-based Internet sports book, the evidence established that over the course of one fifteen month period (when the business was just getting off the ground), Americans wire-transferred in excess of $4.8 million to the sports book in order to wager, and that the sports book was already sizeable (and profitable) enough to accept a $10,000 wager on the outcome of a single football game. *United States v. Jay Cohen,* No. 98 Cr. 434 (S.D.N.Y. 1998)

III. The Statute

A. Section 1084(a)

Known colloquially as the "Wire Wager Act," Title 18, United States Code, Section 1084(a) provides that:

> Whoever being engaged in the business of betting or wagering knowingly uses a wire communication facility for the transmission in interstate or foreign commerce of bets or wagers, or information assisting in the placement of bets or wagers on any sporting event or contest, or for the transmission of a wire communication which entitles the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placing of bets or wagers, shall be fined under this title or imprisoned not more than two years or both.

The purpose of the statute is two-fold:

> (1)to assist the various States and the District of Columbia in the enforcement of their laws pertaining to gambling, bookmaking, and like offenses and [(2)] to aid in the suppression of organized gambling activities by prohibiting the use of wire communication facilities which are or will be used for the transmission of bets or wagers and gambling information in interstate and foreign commerce.

United States v. McDonough, 835 F.2d 1103, 1105 n.7 (5th Cir. 1988) (quoting legislative history). Section 1084, which was enacted in 1961 as part of a series of anti-racketeering laws, compliments other federal anti-bookmaking statutes. See e.g., 18 U.S.C. § 1952 (interstate travel in aid of racketeering enterprises (including enterprises involving gambling)), 18 U.S.C. § 1953 (interstate transportation of wagering paraphernalia), and 18 U.S.C. § 1955 (prohibiting operation of illegal gambling businesses).

In order to establish a violation of Section 1084(a), the government must prove four things:

First, that the defendant was engaged in the business of betting or wagering — in other words, that unlike a casual bettor, he or she derived all or much of his income from the business of gambling. Thus, the statute typically has been enforced against bookmakers and those that work for bookmakers in connection with taking bets or wagers on sporting events or contests.

Second, that the defendant transmitted, in interstate or foreign commerce, any one of the following types of material: (a) bets or wagers; (b) information assisting in the placement of bets or wagers; or (c) a communication that entitled the recipient to receive money or credit as a result of the bet or wager.

Third, that the defendant used a "wire communication facility" to transmit these materials. A "wire communication facility" is defined in Section 1081 as:

> any and all instrumentalities, personnel, services (among other things, the receipt, forwarding, or delivery of communications) used or useful in the transmission of writings, signs, pictures, and sounds of all kind by aid of wire, cable, or other like connection between the points of origin and reception of such transmission.

Fourth, that the defendant acted "knowingly." Under prevailing caselaw, the defendant need not be shown to have known that he or she was violating the law. All that must be shown is that

he or she knowingly, and not by accident or mistake, used a wire communications facility to engage in any one of the three prohibited forms of transmissions described.

B. Section 1084(b)'s Safe Harbor

Subsection (b) of Section 1084 provides two narrow exceptions to the prohibition imposed by Section 1084(a) on the foreign or interstate transmission of material in furtherance of a sports betting business. Subsection (b) provides that:

> Nothing contained in this section shall be construed to prevent the transmission in interstate or foreign commerce of information [(1)] for use in news reporting of sporting events or contests, or [(2)] for the transmission of information assisting in the placing of bets and wagers on a sporting event or contest from a State or foreign country where betting on that sporting event or contest is legal into a State or foreign country in which such betting is legal.

The first exemption was designed to permit "bona fide news reporting of sporting events or contests." H.R. Rep. No. 967, 87th Cong., 1st. Sess. (1961), *reprinted in* 1961 U.S.C.C.A.N. 2631, 2632. The second exception — under which Internet sports book operators frequently seek protection — was created for the discrete purpose of permitting the transmission of *information* relating to betting on particular sports where such betting was legal in both the state from which the information was sent and the state in which it was received. *See, e.g., Sterling Suffolk Racecourse Ltd. v. Burrillville Racing Ass'n*, 989 F.2d 1266, 1272-73 (1st Cir. 1993) (noting that "[t]he legislative history of section 1084 shows beyond peradventure that Congress enacted section 1084(b) for the express purpose of allowing off-track betting in venues where states chose to legalize such activity"). To fall within this aspect of the safe harbor two things must be established: (1) that only "information" was transmitted, and (2) that it was "legal" under the laws of the relevant states to place a bet on that sporting event in the jurisdiction from which the information was sent as well as the jurisdiction in which the information was received.

As the House Report which accompanied the introduction of Section 1084 explained, the second exemption was intended to permit "the transmission of gambling information on a horserace from a State where betting on that horserace is legal to a State where betting on that same horserace is legal." H.R. Rep. No. 967, 87th Cong., 1st. Sess. (1961), *reprinted in* 1961 U.S.C.C.A.N. 2631, 2632. Thus, Congress did not want to criminalize the transmission of information relating to horse races in New York to bettors in Nevada. *See id.* at 2632-33. The information, however, could not legally flow the other way. Because it was illegal under New York law to place a bet in New York on a horse race held in Nevada, this form of transmission fell outside the exemption contained in Section 1084(b). *See id.* at 2632.

It is important to remember, however, that the exemption *only* applies to "information assisting in the placing of bets and wagers on a sporting event or contest," and not to the other two categories of material to which Section 1084(a) applies: the "bets or wagers" themselves, or "communications which entitle the recipients to receive money or credit as a result of bets or wagers." 18 U.S.C. § 1084. *See McDonough,* 835 F.2d at 1105 ("'[n]othing in the exemption . . . will permit the transmission of *bets and wagers* . . . from or to any State, whether betting is legal in that State or not.'") (quoting legislative history).

IV. Defenses Raised To Enforcement And Why They Fail

Against the backdrop of a clearly new technology — the Internet — and a law concededly passed at a time when the Internet did not exist, a number of offshore Internet sports book operators charged under Section 1084(a) have claimed that the statute does not criminalize their bookmaking activities. Challenging prosecutions that have been brought in several districts, they have asserted numerous defenses which, while having superficial appeal, ultimately fail to withstand scrutiny. These arguments include the following:

A. Lack of Extraterritorial Jurisdiction

A number of sports book operators have argued that they are immune because their conduct occurs entirely offshore. Arguing that their offices and employees as well as the computer servers that host their websites and record the bets are all physically located in other countries, defendants have claimed that when Americans access their websites, they make a "virtual visit" to the foreign country. Since sports betting is legal there, the argument continues, the Internet sports book is no more illegal than a casino in Nevada which caters to traditional visitors. Indeed, the sports books have argued, their operations are not subject to the regulation of any state or nation because everything occurs in "cyberspace."

While many of these sports books websites are hosted from computers based offshore (although some only purport to be), the notion that a person "travels" to these foreign nations by communicating with computers there is as persuasive as the notion that a person who picks up a telephone and dials a friend in London should first put on a raincoat. Section 1084(a) by its terms regulates transmissions in "interstate and *foreign* commerce," evidencing Congress' desire that the statute apply to conduct which occurs outside the United States but causes effects within the United States. After soliciting bets from Americans and inviting Americans to send them money, the notion that everything has happened "in cyberspace" and not the United States is similarly inaccurate. Tellingly, the idea of "cyberspace" as a discrete physical place comes from a science fiction novel. *See* William Gibson, *Neuromancer* 51 (1985).

Indeed, as one court colorfully stated in rejecting arguments by a lottery operator in Mexico who solicited bets from Texans:

> If pistol or poison takes intended criminal effect from Mexico in the United States, the United States may punish it if it can catch the criminals. The effect in the United States of the act done in Mexico draws to it jurisdiction to punish those who are responsible for it. It may properly be alleged as done in the United States. These mailed lottery receipts and checks are like bullets that hit their mark. . . . Jurisdiction exists from the standpoint of international law.

Horowitz v. United States, 63 F.2d 706, 709 (5th Cir. 1933). Accordingly, the use of the Internet, even from offshore locations, should not defeat application of Section 1084.

B. Legal in Host Country

A number of defendants have also argued that their conduct is expressly lawful under the laws of their host countries. Indeed, several point out, they are required to be licenced by their host governments, and can obtain licences only after allegedly undergoing rigorous screening by regulators in their host countries. Under such circumstances, it is claimed, enforcement of Section 1084(a) is improper. This argument also misses the point, for whether particular conduct is violative of foreign law is not determinative of whether it is violative of United States law. The Supreme Court has noted that even conduct expressly encouraged by foreign governments may violate United States law. *See Hartford Fire Ins. Co. v. California*, 509 U.S. 764, 795 (1993) ("the fact that conduct is lawful in the state in which it took place will not, itself, bar application of the United States antitrust laws, even where the foreign state has a strong policy to permit or encourage such conduct"). Moreover, since ignorance of law is no defense to a Section 1084(a) prosecution, reliance on the legality of conduct under foreign law should be similarly irrelevant. In sum, issues of foreign law have no place in a Section 1084(a) case, and prosecutors bringing such cases would do well to submit an *in limine* motion precluding resort to such a defense at the earliest hint that it may be asserted.

C. No "Transmission"

A number of defendants have argued that because Section 1084(a)'s reference to precluded transmissions applies only to communications initiated by the sports book, Internet sports books do not engage in prohibited transmissions since they merely make their websites available for viewing by the bettors, who take a "snapshot" of what is on the computer server hosting the website. This argument is also invalid because it

ignores the fundamental technology of how the Internet is used to access computer websites. Simply put, that access involves a continual stream of two-way data transfers between the computers which support the website and the computer used by the person viewing the site. *See Minnesota v. Granite Gate Resorts*, 1996 WL 767431, at *9 (D. Minn. Dec. 11, 1996) (noting that if Internet sports book "did not send an electronic transmission back to the [Minnesota] computer user, the computer user would see nothing. He or she would see a blank screen.")

Additionally, every circuit to have considered the issue, save one, has held that "transmission" as used in Section 1084(a) involves both the sending and the receipt of communications by the bettor. The one Circuit to hold otherwise, *United States v. Stonehouse*, 452 F.2d 455, 456 (7th Cir. 1971), involved a defendant's receipt of a western Union wire ticker — a form of communication intrinsically limited to one-way communications of data.

D. No "Bets or Wagers" Transmitted

Another common argument raised by Internet sports book operators is that their system of wagering, which requires betting from pre-funded wagering accounts and not on credit, somehow distinguishes their operations from the operation of traditional bookies who operate on credit. According to this argument, instructions to wager a specific amount of money on the outcome of a specific game constitute merely "information assisting in the placement of bets," with the transmission of the bets themselves being done entirely in the foreign nation by employees of the bookmaker acting as "agents" for the bettor. Because it is not a crime under the laws of many States to place a sports bet with a bookie, this argument posits that both requirements of Section 1084(b)'s safe harbor are therefore met when a person in a state where betting is not a crime wagers money from a pre-funded account with a bookmaker in a foreign nation where betting is legal. Of course, some state statutes do permit off-track horse wagering, and authorize such wagering based on the distinction between wagering on credit and wagering from pre-funded accounts (so-called "account wagering"). The problem for sports book operators who make this argument, however, is that Section 1084 makes no such distinction. Rather, Section 1084(a) prohibits the transmission of bets and wagers regardless of how the bookie and bettor structure their financial relationship. *See United States v. Ross*, 1999 WL 782749 (S.D.N.Y. Sep. 16, 1999), at *7. It would be absurd to think that Congress meant to make an entire class of transaction otherwise criminalized by Section 1084(a) dependent upon whether a bookie operated on credit or required cash-up-front from the bettor. *See id*.

In sum, while the statute specifically does not define what constitutes a "bet" or "wager," that lack of definition only means that a court should use the common and ordinary meaning of the term. The only reported case to do so has, not surprisingly, held that a bet or wager is transmitted when a person picks up a telephone (or accesses a computer connected to the Internet) and stakes a specific sum of money on the outcome of a specific sporting event. *See Ross*, 1999 WL 782749, at *5-7.

E. Betting is Legal in State in Question

Finally, seizing upon the fact that some states do not make it a crime for a bettor to place a sports bet, a number of sports book operators have attempted to satisfy this requirement of the Section 1084(b) safe harbor by arguing that the only betting that does not qualify for the safe harbor is betting that is made criminal under state law. This argument also should be unavailing, for while it is true that placing a bet (without more) may not be a crime under state law, many states still prohibit such betting. *See, e.g.*, N.Y. Const. Art. I, § 9 (prohibiting all betting not specifically authorized by the legislature); N.Y. Gen. Oblig. Law § 5-401 (all betting not expressly authorized by the legislature made "unlawful"). Once again, common sense understanding of the terms used in the statute should apply, and betting does not become "legal" simply because it is not made criminal.

V. Conclusion

Many of the challenges to Section 1084(a) prosecutions will likely be, or at least should be, resolved prior to trial. Consideration beforehand

of those issues that frequently arise as defenses to prosecutions of Internet sports books will equip a prosecutor to explain to a court and, ultimately, to a jury, why the novelty of the medium does not translate into lack of enforceability. ˜

ABOUT THE AUTHOR

‘ **Joseph V. DeMarco** has been an Assistant United States Attorney in the Southern District of New York since 1997, where he serves as Computer and Telecommunications Crimes Coordinator. Currently, he is on detail to the Department's Computer Crime and Intellectual Property Section (CCIPS).a

Working with Victims of Computer Network Hacks

Richard P. Salgado
Trial Attorney
Computer Crime and Intellectual Property Section

In our ten years' experience in detecting, locating, and prosecuting network intruders (hackers) we have seen that, as with many offline crimes, robust law enforcement alone cannot solve the network intruder problem. To be effective, any overall strategy must include the owners and operators of the nation's computer networks. They are the first line of defense and have the responsibility to take reasonable measures to ensure that their systems are secure. They are also in the best position to detect intrusions and take the first critical steps to respond. At the most basic level, we rely on network operators to report to us when their systems are hacked. Intrusion victims, however, are often even more reluctant to call law enforcement than other business victims. This reluctance has been reflected in the surveys conducted jointly by the Computer Security Institute and the FBI. In the year 2000 survey, for example, only 25% of the respondents who experienced computer intrusions reported the incidents to law enforcement. To better understand why and to learn how we can promote reporting, the Department of Justice has undertaken a concerted effort to reach out to the operators of our nation's computer networks.

As part of this effort, the Department, through the Computer Crime and Intellectual Property Section, has participated with the Information Technology Association of America in several industry-government summits this past year. The first two summits (held in Palo Alto, California, and Herndon, Virginia, respectively) were national in scope. Several regional summits followed, with more in the planning. The discussions in the summits concentrated on how law enforcement and victims of computer intrusions could work better together. Although several larger themes common to all the summits became apparent, one theme of particular concern was that private victims of computer network intrusions are reluctant to report the crimes to law enforcement.

The reluctance of intrusion victims to report poses a significant problem to the development of networked computers generally, and the Internet in particular. Although, upon finding a hacker in his or her system, a system administrator may be content to close the intruder's account and fix the vulnerability (essentially kicking the hacker out and locking the door), this provides little true security. Not only is the hacker free to try the exploit on another company's network, the hacker may have left behind back doors through which he or she can return to the computer undetected. In addition, through the hacker community, others may learn of the exploit and, emboldened by the

lack of any law enforcement response, join in compromising computer systems. It is folly to believe that any particular hacker is motivated by the desire to show-off computing prowess with no real intent to damage, steal, or defraud. What may appear to be a simple hack with no real risk of damage can, in fact, be a part of a larger scheme to launch a very destructive attack against other highly sensitive machines. Intruders may compromise many systems, collecting them like baseball cards. Some hackers use the "stolen" computers to launch attacks against other computers, shutting down the next victim, taking information from the systems, and using the stolen data in extortion schemes, or to engage in innumerable other types of illegal conduct. With each compromise, the security of our nation's networks diminishes. Without reporting by victims, law enforcement cannot provide an effective and appropriate response.

Myths and Misunderstandings

During the summits, some of the industry participants claimed a wide variety of reasons for the reluctance to report hacks. The perception on the part of some businesses is that there is little upside to reporting network intrusions. The perceived rationale for not reporting an intrusion include the following:

- The victim company does not know which law enforcement entity to call. Surely, the victim reasons, the local or state police will not be able to comprehend the crime and the FBI and Secret Service would have no interest in my system.
- If the victim company does report the intrusion to an appropriate agency, law enforcement will not act. Instead, the fact of the intrusion will become public knowledge, irreparably shaking investor confidence and driving current and potential customers to competitors who elect not to report intrusions.
- If law enforcement does act on the report and conducts an investigation, law enforcement will not find the intruder. In the process, however, the company will lose control of the investigation. Law enforcement agents will seize critical data, and perhaps entire computers, damage equipment and files, compromise private information belonging to customers and vendors, and seriously jeopardize the normal operations of the company. Only competitors will benefit as customers flee and stock value drops.
- If law enforcement finds the intruder, the intruder likely will be a juvenile, reside in a foreign country, or both, and the prosecutor will decline or be unable to pursue the case.
- If the intruder is not a minor, the prosecutor will conclude that the amount of damage inflicted by the intruder is too small to justify prosecution.
- If law enforcement successfully prosecutes the intruder, the intruder will receive probation or at most insignificant jail time, only to use his or her hacker experience to find fame and a lucrative job in network security.

As formidable as the list of excuses may appear, these deterrents to reporting can be overcome by better-informed computer network owners and operators, and skillful investigatory and prosecutorial practice. Further, the risk presented by failing to report intrusions is tremendous. For the foreseeable future, our nation's networks are only going to get more complex, more interconnected and thus more vulnerable to intrusions. Networks are also going to be more important to our private lives, the nation's defense, and our world's economy. If there was a single clear mandate from the summits, it was that we must get the word out explaining why victims should report intrusions.

The Case for Reporting

Law enforcement needs to debunk the myths that have developed about the dangers of reporting intrusions and to sharpen our investigatory and prosecutorial practices. We also need to make an affirmative case for reporting to large network computer operators, focusing on the value to the company of reporting. In the course of the summits, it became clear that the message to operators and owners of computer networks is best delivered before a crises arises, when

relationships can be built without the pressure of an ongoing investigation.

Debunking the Myths and Explaining the Basics

Perhaps the most basic piece of information to convey to victims concerns to whom the victim should report. Law enforcement agencies at all levels have developed some familiarity with computer crime investigations in the recent years, and if they are not equipped to handle complex computer intrusion cases, they are at least able to promptly refer reports to agencies that are. We need to ensure that large computer network operators know the law enforcement agencies in their area that have the necessary forensic and prosecutorial expertise and resources. Victims also need to understand that law enforcement does view intrusions as important and will respond appropriately.

Publicity that may follow reporting was also a concern that pervaded the summits. As a rule, agents and prosecutors need to ensure that they handle business information with a great deal of discretion. Similarly, law enforcement has to be sensitive to victims' concerns arising from the seizure of data from internal corporate networks. Most of the industry participants in the summits thought that law enforcement investigators would remove the servers, proceed without any victim input, that it would disrupt the normal operations of the company for weeks at a time, and that law enforcement's involvement would mean that the company could not take steps to secure the system or conduct its own investigation. Contrary to this belief, many investigations actually require input from the victim's system operator for technical operations. Communication with potential victims prior to any investigation would likely go a long way to address these concerns. Similarly, during investigations, law enforcement can work with the victims to ensure that the investigation remains confidential.

Certainly every investigation poses its own unique challenges, and there is no way to predict, with certainty, how any particular investigation will proceed. We have seen, and undoubtedly will see again, instances where a victim wants to take measures that are in conflict with the investigative strategy. For example, where there is a series of intrusions into a victim's network, the victim may want to shut the intruder out of the system and patch the vulnerability. Law enforcement may prefer that the company leave the system open so that the hacker will not know he or she has been detected, and the agents can monitor the hacker's activity and track the hacker's origins. If there is a cooperative and trusting relationship between law enforcement and the victim that predates the intrusion, the agents and the company are more likely to find a resolution that works for both. In this example, the agents and system operator may be able to configure the network such that it is secure against future exploits, but appears to the hacker to remain open. Law enforcement can both protect the victim and pursue the intruder.

Many of the industry representatives expressed doubt about the ability of law enforcement to find the culprits. Certainly, tracking intruders is a very challenging task for a variety of reasons. Industry representatives readily acknowledged, however, that intruders will not be caught if the victim does not report. In any event, law enforcement has become much more sophisticated at tracking communications in recent years and even juvenile intruders are not immune from prosecution. Even if the juvenile is outside the United States, many foreign countries have been willing to prosecute.

Highlighting the Value of Reporting

There are also business reasons for companies to report intrusions cases. The two primary values to victims in calling law enforcement come from the deterrence that prosecution provides and potential restitution to the victim.

Specific deterrence is perhaps one of the most compelling reasons for a company to report an intrusion. When law enforcement catches and successfully prosecutes an intruder, that intruder is deterred from future assaults on the victim. This is a result that no technical fix to the network can duplicate with the same effectiveness. Intrusion victims may try to block out an intruder by fixing the exploited vulnerability, only to find that the intruder has built in a back door and is able to access the system at will. There have been instances in which a system operator, believing he

or she is locking the intruder out for good, expends a great deal of time and effort to completely rebuild the network using backup media, only to find that the exploit was present in the backup and was simply reintroduced. Of course, a victim could initiate its own investigation to find the intruder. If successful, the victim may be able to initiate a civil suit for damages. In many (if not most) cases, however, the victim is at a substantial disadvantage relative to law enforcement in this effort. Law enforcement is able to obtain wiretap, pen/trap and trace orders, enforceable data preservation requests and other criminal process unavailable to a private party. Further, a monetary award is unlikely to serve as the same deterrent as a jail sentence or even probation. The general deterrence that criminal law enforcement provides also benefits victims and potential victims in the long run.

Restitution is also an attractive motive for victim reporting. Being a victim of intrusion is almost always an expensive proposition. A responsible victim must survey the system to determine whether any data was taken or damaged, and if so must repair the damage. The victim must analyze the network to determine if there are any remaining holes in the system, check the integrity of the logs, identify the means by which the intruder accessed the system, and patch the vulnerability. The costs can be very high, and can grow when the victim includes the loss of business and the lost productivity of the technical staff dedicated to the intrusion. The victim may be able to recoup some or all of the expenses through restitution.

Reporting a criminal computer intrusion to law enforcement may also help the victim recover under insurance policies for damage to its system or damage inflicted on a third party resulting from the intrusion. Director and Officer insurance policies, for example, may exclude coverage if as a result of the victim's decision not to report the intrusion to law enforcement, the intruder inflicted additional damage to the victim system or attacked another's network using the victim's system. By reporting the intrusion in the first instance, however, the victim decreases the risk that the carrier could deny a claim made.

Similarly, where a victim's network is compromised and used to attack another system downstream, the victim may find itself a defendant in civil litigation brought by that downstream victim. If the victim has reported to law enforcement, it will be able to use the fact that it called in law enforcement as part of its defense of a claim, for example, that the victim did not take reasonable steps to prevent its network from being used as a platform to attack the plaintiff.

Making the Case and Selecting the Appropriate Audience

The summits illustrated that informal face-to-face meetings between law enforcement and representatives of potential intrusion victims is a valuable means to address concerns that the victims may have about reporting. Those industry representatives at the summits that had pre-existing relationships with law enforcement almost uniformly expressed an understanding of the need to report intrusions, and a willingness to do so. Those most reluctant to report, it appeared from the summits, were representatives who had no such relationship. Discussions in the heat of an investigation are far less likely to be productive than frank and informal dialogue prior to an incident. Prosecutors and agents should take the time to reach out to the large computer operators in their jurisdictions and build such relationships.

It is imperative that the message is heard by those who make the decisions. Some information security (IS) managers, for example, are very protective of "their" systems and will take umbrage at intrusions. They may not be content with simply re-securing the system in the hope that the hacker will not return, and will want the criminal arrested and prosecuted. They view law enforcement as a part of their security system; one of many resources that responsible network operators will use when the security of the network has been compromised. Other IS managers may be less receptive to reporting intrusions, even to their own superiors. The very fact of an intrusion, an IS manager may fear, suggests that he or she failed to properly secure the system. It has also become common for law enforcement to receive hacking reports from IS managers, but receive less than enthusiastic

cooperation from the victim company once the fact of the hack is brought to the attention of the victim's higher-level management or general counsel. For the message to be effective, it must be heard by all the decision makers.

To get the word out, prosecutors and agents should take the time to reach out to the large computer operators in their jurisdictions. In addition to meeting with representatives of information technology companies such as Internet and telecommunications service providers, agents and prosecutors should look to other common targets of hacks including universities, e-commerce and web-based retailers, and any organization that is reliant on large computer networks for operations. In addition, many jurisdictions are the home for information security associations, computer technology bar associations, and similar organizations. Those groups can provide law enforcement a solid forum in which to reach many network operators and counselors. The Computer Crime and Intellectual Property Section can help in this effort.

The perception that law enforcement and private computer network operators have separate and independent responsibilities in the battle against hackers is wrong. Although the network owners have the obligation to secure their systems, and law enforcement has an obligation to investigate and prosecute when appropriate, neither can function effectively without the other. Network operators need to view law enforcement as a necessary part of system protection, and law enforcement agencies need to be able to count on the cooperation of victims to fulfill their responsibilities. ~

ABOUT THE AUTHOR

‘ **Richard P. Salgado** is a trial attorney in the Computer Crime and Intellectual Property Section of the Criminal Division of the United States Department of Justice. In that role, he addresses a wide variety of complex legal and policy issues that arise in connection with new technologies. His responsibilities include training investigators and prosecutors on the legal and policy implications of emerging technologies and related criminal conduct. Mr. Salgado also prosecutes and provides advice on computer hacking and network attacks, and other advanced technology crimes including denial of service attacks, logic bombs, viruses and computer extortion, wiretaps and other technology-driven privacy crimes. Mr. Salgado also participates in policy development relating to emerging technologies, and in the Department's computer crime industry outreach efforts. Mr. Salgado has also served as lead negotiator on behalf of the Department in discussions with communications service providers to ensure that the ability of the Department to enforce the laws and protect national security is not hindered by foreign ownership of the providers or foreign located facilities.**a**

Supervised Release and Probation Restrictions In Hacker Cases

Christopher M.E. Painter
Deputy Chief, Computer Crime and Intellectual Property Section

An often overlooked aspect of sentencing in computer crime cases are conditions that the court can impose as part of a sentence of probation or supervised release. These conditions can be tailored to restrict, among other things, a defendant's employment, associations, and other activities, once he is released from any term of imprisonment the court imposes to protect the public and aid in a defendant's rehabilitation. Such conditions are routinely imposed in non-computer crime cases. For example, in bank fraud cases or insurance fraud cases, courts often impose conditions restricting a defendant's employment in those industries. In investment fraud cases, defendants are prohibited from handling other people's money and in telemarketing cases, courts have prohibited defendants from soliciting investors, using names other than their own and have even restricted their access to telephones.

Appropriate restrictive supervised release conditions are even more important in hacker cases. In many hacker cases, the defendants have engaged in illegal conduct over a protracted period, are recidivists, or have otherwise demonstrated that they are unlikely to refrain from illegal hacking even after a conviction or imprisonment. In these cases, restrictive conditions that proscribe certain kinds of otherwise lawful conduct, such as use of aliases, association with other hackers, or, in extreme cases, access to computers and computer networks, serve to protect the public. This is particularly true when the sentence of imprisonment is either relatively short or where probation is imposed, despite the destructiveness of a defendant's conduct, or because the full extent of a defendant's activities is not determined. In other cases, particularly where the defendant is young, there is a good chance of rehabilitation. In these cases, supervised release or probation conditions can aid a defendant's rehabilitation by controlling or monitoring his access to those things that have tempted him in the past. In either case, appropriately tailored conditions can aid the probation office and the court in monitoring a defendant's conduct for the period of supervised release or probation to ensure he does not engage in further illegal conduct. If a defendant violates those conditions, the probation officer can seek revocation or modification of supervised release or probation and the court can impose additional imprisonment or refine the restrictions on the defendant's conduct.

In general, in addition to certain mandatory conditions of supervised release, the court may order "any other condition it considers to be appropriate" so long as the conditions are "reasonably related" to the factors set forth in 18 U.S.C. §§ 3553(a)(a), (1)(2)(B), (a)(2)(C), and (a)(2)(D). 18 U.S.C. § 3583(d). Specifically, conditions of the release must be reasonably related to the following factors:

- the nature and circumstances of the offense and the history and characteristics of the defendant; and
- the need for the sentence imposed – (B) . . . to afford adequate deterrence to criminal conduct; (C) to protect the public from further crimes of the defendant; and (D) to provide the defendant with needed educational or vocational training, medical care, or other corrective, treatment in the most effective manner. 18 U.S.C. § 3553.

See also United States Sentencing Guidelines ("U.S.S.G") § 5D1.3(b). The probation statute, 18 U.S.C. § 3563, also allows the imposition of discretionary conditions that are related to "the need for the sentence imposed . . . to reflect the seriousness of the offense, to promote respect for

the law, and to provide just punishment for the offense," 18 U.S.C. § 3553(a)(2)(A), whereas the supervised release statute does not. *United States v. Eyer*, 67 F.3d 1386, 1392 n.8 (9th Cir. 1995).

These conditions are not prerequisites, and a court may properly impose a condition of supervised release that is reasonably related to only some of these factors. *United States v. Johnson*, 998 F.2d 696, 697-98 (9th Cir. 1993). The conditions must also involve no greater deprivation of liberty than is reasonably necessary for the purposes set forth above. 18 U.S.C. § 3583(d). Furthermore, the conditions must be consistent with pertinent policy statements issued by the Sentencing Commission. *Id*. In setting conditions, including those "restricting fundamental rights," the sentencing court has broad discretion. *United States v. Bolinger*, 940 F.2d 478, 480-81 (9th Cir. 1991).

U.S.S.G. § 5F1.5 allows a court to impose a condition of supervised release restricting employment in a specified occupation, business, or profession if it determines that:

- a reasonably direct relationship existed between the defendant's occupation, business, or profession and the conduct relevant to the offense of conviction; and
- imposition of such a restriction is reasonably necessary to protect the public because there is reason to believe that, absent such restriction, the defendant will continue to engage in unlawful conduct similar to that for which the defendant was convicted.

That section also states that "[i]f the court decides to impose a condition of probation or supervised release restricting a defendant's engagement in a specified occupation, business, or profession, the court shall impose the condition for the minimum time and to the minimum extent necessary to protect the public." *Id.*

The range of permissible discretionary conditions a court can impose is exceptionally broad and permits a wide range of restrictions depending on the facts of an individual case and the history and prospects of the defendant. In a first-time hacker case, the restrictions could be as simple as a prohibition against unauthorized use of computer systems, a prohibition against association with others who have engaged in illegal hacking activities, and a directive that defendant use his own name when communicating online. On the other side of the spectrum, much broader conditions may be warranted.

For example, in the prosecution of the prolific and notorious computer hacker Kevin Mitnick, the court imposed the following conditions as part of his sentence:

> Without the prior express written approval of the probation officer:
>
> - The defendant shall not possess or use, for any purpose, the following:
>   - Any computer hardware equipment;
>   - Any computer software programs;
>   - Modems;
>   - Any computer related peripheral or support equipment;
>   - Portable laptop computers, "personal information assistants," and derivatives;
>   - Cellular telephones;
>   - Televisions or other instruments of communication equipped with on-line, Internet, world-wide web, or other computer network access;
>   - Any other electronic equipment, presently available or new technology that becomes available, that can be converted to or has as its function the ability to act as a computer system or to access a computer system, computer network or telecommunications network

(except defendant may possess a "land line" telephone);

- The defendant shall not be employed in or perform services for any entity engaged in the computer, computer software, or telecommunications business and shall not be in any capacity wherein he has access to computers or computer-related equipment or software;
- The defendant shall not access computers, computer networks, or other forms of wireless communications himself or through third parties;
- The defendant shall not act as a consultant or advisor to individuals or groups engaged in any computer-related activity;
- The defendant shall not acquire or possess any computer codes (including computer passwords), cellular phone access codes, or other access devices that enable the defendant to use, acquire, exchange, or alter information in a computer or telecommunications database system;
- The defendant shall not use or possess any data encryption device, program or technique for computers;
- The defendant shall not alter or possess any altered telephone, telephone equipment, or any other communications-related equipment;
- The defendant shall only use his true name and not use any alias or other false identity.

These conditions that both restrict defendant's access to computers, computer networks, and cellular phones and restrict his employment in the computer or telecommunications industries, were justified and necessitated by defendant's habitual hacking activities and long history of failing to obey court-ordered restrictions on his conduct. Mitnick engaged in criminal hacking and telecommunications fraud from the time he was a juvenile. In 1988, after several state convictions and revocations of probation for computer fraud, defendant was charged and pled guilty in federal court for hacking into Digital Equipment Corporation computers, stealing proprietary software, and using unauthorized access devices. He was sentenced to twelve months in prison followed by a three year period of supervised release. The judge imposed straightforward conditions of supervised release prohibiting Mitnick from engaging in further illegal access into computer or telecommunications networks and prohibiting him from associating with others known to have engaged in such conduct. Nevertheless, near the end of his supervised release term, Mitnick hacked into Pacific Bell voice mail computers and associated in this endeavor with another individual (and later co-conspirator) who had previously been convicted of computer fraud.

A warrant was issued for Mitnick's arrest and he fled, becoming a fugitive for the next two and one half years. During this time, Mitnick engaged in a virtual "hacking spree" gaining unauthorized access to dozens of computer networks using cloned cellular phones to hide his location and, among other things, stealing valuable proprietary software from some of the country's largest cellular telephone and computer companies. Mitnick also intercepted and stole computer passwords, altered computer networks, and broke into and read private e-mail. Mitnick was apprehended in February 1995 in North Carolina. When arrested he was found with cloned cellular phones, over one hundred clone cellular phone codes, and multiple pieces of false identification.

In imposing the extensive conditions of supervised release, the judge held a number of hearings and based her ruling on defendant's long history of hacking, defendant's inability to comply with less onerous restrictions and, most importantly, the need to protect the public. The court's focus on the "tools" Mitnick has habitually

used to commit past criminal conduct, computer and cellular phones, was wholly appropriate given defendant's seeming inability to use these tools in a law-abiding manner. Given his past extensive and repeated criminal conduct, and the prospect that, unsupervised, he would be tempted to engage in the conduct again, the court expressly stated that the conditions were designed to protect the community. The court's occupational restrictions prohibiting his employment in the computer and telecommunications industries were similarly designed primarily to protect the public from future illegal conduct by removing both the tools Mitnick could use to commit this conduct and the tools that might tempt him to further transgressions.

Of course, conditions as broad as the ones imposed in the *Mitnick* case must be justified by the facts of the case at issue. If such conditions are justified by a defendant's history and the nature of the offense, and if the judge makes an adequate record to support his or her findings, they should survive any challenge raised on appeal. Common challenges to conditions of supervised release restricting a defendant's association and activities are that such restrictions impermissibly restrict otherwise legal activities, that they violate the defendant's First Amendment rights, or are impermissibly vague or ambiguous. Mitnick challenged the conditions imposed by the court on each of these grounds but was flatly rejected by the Ninth Circuit Court of Appeals. *United States v. Kevin Mitnick*, No. 97-50365, 1998 WL255343 (9th Cir. May 20, 1998).

The argument that broad supervised release conditions restrict otherwise lawful activity misses the point. Courts have frequently curtailed activities that, though otherwise legitimate, nevertheless might tempt a defendant to engage in further illegal conduct. *See United States v. Lowe*, 654 F.2d 562, 566 (9th Cir. 1981) (court could properly restrict access within 250 feet of military base, thereby effectively precluding legitimate leafleting activity, to remove temptation of separate criminal conduct – trespassing on base); *United States v. Bolinger*, 940 F.2d 478, 480 (9th Cir. 1991) ("Probation conditions may seek to prevent reversion into former crime-inducing lifestyle by barring contact with old haunts and associates, even though the activities may be legal"); *United States v. Peete*, 919 F.2d 1168, 1181 (6th Cir. 1990) (proper to prohibit defendant convicted of violating Hobbs Act from running for public office to insulate him from temptation of same environment and protect the public); *United States v. Turner*, 44 F.3d 900, 903 (10th Cir. 1995), (court properly ordered defendant not to picket abortion clinics because "it is not too fantastic to speculate that if she were permitted to protest at an abortion clinic she might not be able to restrict her activities within lawful parameter"); *United States v. Choate*, 101 F.3d 562, 566 (8th Cir. 1996) (defendant properly prohibited from self-employment because of risk that prior "excesses of salesmanship" could again lead to illegal conduct if not supervised).

In *Malone v. United States*, 502 F.2d 554 (9th Cir. 1974), defendant was convicted of unlawful exportation of firearms to Ireland and, as part of his sentence, was ordered not to associate with, or belong to, any Irish organization, group, or movement, not to be employed in any capacity that directly or indirectly associated him with such groups and not to visit any Irish pubs. *Id.* at 555. In upholding these restrictions, the court recognized that the incidental chance of temptation warranted these conditions despite their usually lawful character:

> The conditions here involved are not intended to infer that each member of a group or organization with which the appellant is forbidden to associate will necessarily lead him into criminal activities or be a bad influence. It is the incidental association with one or more who might lead him to future criminality that the court seeks to prevent. If the trial judge could only prohibit active association with a group having an illegal purpose, then the court would be, in effect, restricted to the standard condition that the probationer obey the law. It does not appear such limitation was intended. Here the crime stemmed from high emotional involvement with Irish Republic sympathizers.

Id at 556.

Challenges based on an impermissible restriction of a defendant's rights of expression or

association should be similarly unavailing. Despite the growing importance of the Internet as a means of communication, restrictions on access to that technology are proper if related to and reasonably necessary to promote the goals of sentencing. It is axiomatic that those convicted of criminal conduct are "properly subject to limitations from which ordinary citizens are free[.]" *United States v. Consuelo-Gonzalez*, 521 F.2d 259, 265 (9th Cir. 1975). Accordingly, the district court retains its broad discretion in setting conditions of supervised release and probation, even where fundamental rights are involved. *Bolinger*, 940 F.2d at 480. Although conditions restricting fundamental rights are reviewed carefully, *Lowe*, 654 F.2d at 567, there is no "presumption, however weak, that such limitations are impermissible". *Consuelo-Gonzalez*, 521 F.2d at 265. As the Ninth Circuit stated in *Consuelo-Gonzalez*:

> Merely because a convicted individual's fundamental rights are involved should not make a probation condition which limits those rights automatically suspect. The development of a sensible probationary system necessarily requires that the trial court be vested with broad discretionary powers. It also requires that any condition which is imposed following conviction, whether or not it touches upon "preferred" rights, must be viewed in the context of the goals underlying the Act. Thus, the crucial determination in testing probationary conditions is not the degree of "preference" which may be accorded those rights limited by the condition, but rather whether the limitations are primarily designed to affect the rehabilitation of the probationer or insure the protection of the public.

Consuelo-Gonzalez, 521 F.2d at 265 n.14. The restriction of even "preferred rights" is valid so long as they are: "(1) primarily designed to meet the ends of rehabilitation and protection of the public and (2) reasonably related to those ends." *Bolinger*, 940 F.2d at 480. Like any other special condition of supervised release, such conditions also must involve no greater deprivation of liberty than is reasonably necessary. 18 U.S.C. § 3583(d).

Courts have routinely deferred to the sentencing court's broad discretion in setting conditions notwithstanding the implication of fundamental rights. *See, e.g.*, *Malone*, 502 F.2d at 556 (upholding restrictions limiting association with all Irish groups against First Amendment claim); *Lowe*, 654 F.2d at 566-67 (upholding conditions that effectively precluded defendants from distributing literature to employees of military base or attend certain weekly meetings against free speech and association claim); *Peete*, 919 F.2d at 1118 (prohibition on holding public office upheld); *United States v. Bird*, 124 F.3d 667, 684 (5th Cir. 1997) (rejecting First Amendment challenge to condition that defendant stay 1,000 feet away from abortion clinics where he had previously been convicted for trespassing at abortion clinics); *United States v. Showalter*, 933 F.2d 573, 575 (7th Cir. 1991) (conditions upheld requiring the defendant convicted of possession of unregistered firearm to avoid associating with other skinheads and neo-Nazis).

As long as restrictions are reasonably related to the offense and defendant's history, are primarily designed to protect the public and promote rehabilitation by preventing recidivism, are expressly related to those ends, and particularly in light of defendant's past conduct, involve no greater deprivation of liberty than is reasonably necessary to achieving those ends, they should survive a First Amendment challenge.

A final likely claim is that broad conditions restricting access to computers are fatally vague and overbroad. Mitnick, for example, argued that because almost everything from automobiles to ATMs and toasters include computer chips, he would be forced to live as a hermit or commit unintentional violations of supervised release. Both the District Court and Court of Appeals rejected this argument stating that conditions restricting computer access should be read in a common sense manner. Although due process requires a defendant to be given fair warning before he forfeits his liberty, *see United States v. Grant*, 816 F.2d 440, 442 (9th Cir. 1987).

> [f]air warning is not to be confused with the fullest or most pertinacious, warning imaginable. Conditions of probation do not

> have to be cast in letters six feet high, or to describe every possible permutation, or spell out every last self-evident detail [they] may afford fair warning even if not precise to the point of pedantry. In short, conditions of probation can be written – and must be read in a common sense way.

United States v. Gallo, 20 F.3d 7, 11 (1st Cir. 1994). (internal citations omitted)

The scope and detail of supervised release restrictions in hacker cases will be highly dependent on the facts of the particular case and the history of the defendant. Nevertheless, prosecutors should be aware these conditions can be used as a powerful tool to protect the public and aid in rehabilitation. Accordingly, prosecutors should consider appropriate conditions when negotiating a plea agreement or in arguments presented during sentencing proceedings. ~

ABOUT THE AUTHOR

‘ **Christopher M.E. Painter** is a Deputy Chief of the Computer Crime and Intellectual Property Section at the Department of Justice. From 1991 to March 2000, Mr. Painter was a criminal prosecutor in the U.S. Attorney’s Office for the Central District of California (Los Angeles). Since taking that post, Mr. Painter specialized in the investigation and prosecution of high-tech, intellectual property and computer crimes and served as a Computer Crime and Internet Fraud Coordinator for his office.

Mr. Painter has investigated and prosecuted some of the most significant and high profile high-tech cases in the country, including the prosecution of notorious computer hacker Kevin Mitnick, the prosecution of the first Internet stock manipulation case involving the posting of a bogus Bloomberg News page falsely reporting the sale of a company called PairGain that caused its stock to soar, prosecution of another internet stock manipulation case, involving former and present UCLA students who hyped stocks on Yahoo by posting false spam messages, and the prosecution of one of the first Internet auction fraud cases. Mr. Painter co-chairs an ABA subcommittee concerning high-tech crimes and serves on several Department of Justice and interagency working groups relating to computer and Internet hackers, Internet fraud investigations and prosecutions, electronic evidence, intellectual property crimes, and thefts of trade secrets. He has frequently lectured to private groups and at the National Advocacy Center, appeared on 60 Minutes, CNN, CBS Morning News, the BBC, and has testified before Congress concerning computer crime issues.a

NOTES

UPCOMING PUBLICATIONS

May 2001 Cybercrime II

July 2001 Tax Issues

Request for Subscription Update

In an effort to provide the UNITED STATES ATTORNEYS' **BULLETIN** to all who wish to receive, we are requesting that you e-mail Nancy Bowman (nancy.bowman@usdoj.gov) with the following information: Name, title, complete address, telephone number, number of copies desired, and e-mail address. If there is more than one person in your office receiving the **BULLETIN**, we ask that you have one receiving contact and make distribution within your organization. If you do not have access to e-mail, please call 803-544-5158. Your cooperation is appreciated.